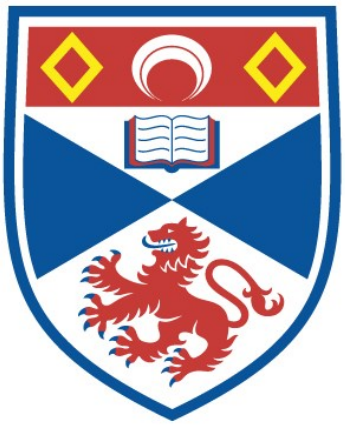
FIBONACCI LENGTH AND EFFICIENCY IN GROUP PRESENTATIONS

Peter Philip Campbell

A Thesis Submitted for the Degree of PhD
at the
University of St Andrews



2003

FIBONACCI LENGTH AND EFFICIENCY IN GROUP PRESENTATIONS

Peter Philip Campbell

Ph.D. Thesis

University of St Andrews

2003

To

my parents

and

"l'amor che move il sole e l'altre stelle."

Contents

Declaration

I, Peter Philip Campbell, hereby certify that this thesis has been written by me, that it is the record of work carried out by me and that it has not been submitted in any previous application for a higher degree.

Name: Peter P. Campbell **Signature:**..... **Date:** 29/4/03

I was admitted as a research student in September 1999 and as a candidate for the degree of Doctor of Philosophy in September 1999; the higher study for which this is a record was carried out in the University of St Andrews between 1999 and 2003.

Name: Peter P. Campbell **Signature:**..... **Date:** 29/4/03.

I hereby certify that the candidate has fulfilled the conditions of the Resolution and Regulations appropriate for the degree of Doctor of Philosophy in the University of St Andrews and that the candidate is qualified to submit this thesis in application for that degree.

Name: Edmund F. Robertson **Signature**..... **Date:** 29/4/03

In submitting this thesis to the University of St Andrews I understand that I am giving permission for it to be made available for use in accordance with the regulations of the University Library for the time being in force, subject to any copyright vested in the work not being affected thereby. I also understand that the title and abstract will be published, and that a copy of the work may be made and supplied to any bona fide library or research worker.

Name: Peter P. Campbell **Signature:**..... **Date:** 29/4/03

Acknowledgements

I would like to take this opportunity to thank all those who have helped me during my time as a PhD student.

Firstly I would like to thank my family who have always helped me when I needed it. I would especially like to mention my mother, father, brother, Janet, Thomas and Charlotte. Saying thank you does not seem enough.

Next I would like to mention Professor E. F. Robertson who gave me guidance and friendship from the first day I arrived in the department. I would also like to thank Doctors C. M. Campbell, N. Ruškuc and H. Doostie who have been instrumental in helping me mature mathematically. Together the above have taught me the truth of the phrase

> It is only by challenging and refining the activity that it can be kept brimfull of meaning, and thus bring profound satisfaction.[44]

I would also like to thank all my friends and colleagues who have known me during this period. They are too numerous to mention here, but they know who they are. I am grateful for having the honour of calling them friends.

Abstract

In this thesis we shall consider two topics that are contained in combinatorial group theory and concern properties of finitely presented groups. The first problem we examine is that of calculating the Fibonacci length of certain families of finitely presented groups. In pursuing this we come across ideas and unsolved problems from number theory. We mainly concentrate on finding the Fibonacci length of powers of dihedral groups, certain Fibonacci groups and a family of metacyclic groups.

The second problem we investigate in this thesis is finding if the group $PGL(2,p)$, for p a prime, is efficient on a minimal generating set. We find various presentations that define $PGL(2,p)$ or $C_2 \times PSL(2,p)$ and direct products of these groups. As in the previous sections we come across number theoretic problems. We also have occasion to use results from tensor theory and homological algebra in order to obtain our results.

Chapter 1

Introduction

In this chapter we will introduce the basic concepts that will be used in subsequent chapters of this thesis. Most of the results here will be from (combinatorial) group theory and will pertain to finitely presented groups. With this in mind we first define a (group) presentation:

1 Group presentations: Theory and procedures

Definition 1.1 Let X be a set, $F(X)$ be the free group on X and $R \subseteq F(X)$. Then a *(group) presentation* is a pair $\langle X \mid R \rangle$.

Having defined a group presentation we now say what is meant for a group to be defined by a given presentation.

Definition 1.2 Let X be a set, $F(X)$ be the free group on X, $R \subseteq F(X)$ and $\overline{R}$ be the normal closure of the set R in $F(X)$, i.e. the subgroup of $F(X)$ generated by the set $\{g^{-1}rg \ : g \in F(X), r \in R\}$. Then the group G is said to be defined by the presentation $\langle X \mid R \rangle$ if $G \cong F(X)/\overline{R}$.

Remark 1.3 As is normal in the literature we will abuse the notation by sometimes writing $G = \langle X \mid R \rangle$. In the definition above, the set R contains only relators i.e. just elements of the free group $F(X)$. In this thesis we will use relators and relations as appropriate, i.e. instead of writing the relator uv, with $u, v \in F(X)$, we may write $uv = 1$ or even $u = v^{-1}$. When rewriting words we use the convention found in [62], namely the use of underscores to highlight the subwords which are replaced in passing from one word to the next.

We say that in a presentation $\langle X \mid R \rangle$ the set X is the set of *generators* and the set R is the set of *relators.*

Definition 1.4 A group G is said to be *finitely presented* if it can be defined by a presentation $\langle X \mid R \rangle$ where both X and R are finite sets.

Remark 1.5 It must be stated here that not all groups possess the finiteness property of being finitely presented. Obviously if G is not finitely generated then it cannot be defined by a finite presentation. An example of such a group is the rationals $\mathbb{Q}$ under the normal addition of rational numbers. On the other hand there are some groups that are finitely generated but cannot be finitely presented. This result follows from the following two theorems:

Theorem 1.6 *There exist* $2^{\aleph_0}$ *nonisomorphic 2-generator groups.*

Proof. See [56] for a, relatively long, proof. □

Theorem 1.7 *There exist only countably many nonisomorphic finitely presented groups.*

Proof. This follows when we consider the possibilities for the number of finite generating and relator sets. □

Giving examples of finitely generated groups that are not finitely presented is rather difficult, as given a finitely presented group G one cannot in general decide if it is finitely presentable or not. A standard example of a finitely generated group that is not finitely presentable is the standard wreath product of two infinite cyclic groups; a rather long and complicated proof may be found in [56].

Example 1.8 The following will be called standard presentations for the named groups:

(1) $\langle\, x \mid x^n = 1 \,\rangle$, the cyclic group of order n,

(2) $\langle\, x, y \mid x^2 = 1, y^n = 1, (xy)^2 = 1 \,\rangle$, the dihedral group of order $2n$,

(3) $\langle\, x, y \mid x^{2^{n-1}} = 1, y^2 = x^{2^{n-2}}, xyx = y \,\rangle$, $n \geq 3$, the generalized quaternion group Q_{2^n}.

The notion of a finitely presentable group is one of the cornerstones of combinatorial group theory. A fundamental theorem within this area is commonly called von Dyck's Lemma:

Lemma 1.9 (von Dyck's Lemma) *Let $F(X)$ be the free group on the set X and let $\overline{R}$ denote the normal closure of the set R in $F(X)$. If $G = \langle\, X \mid R \,\rangle$ and $H = \langle\, X \mid S \,\rangle$, where $R \subseteq S \subseteq F(X)$, then there exists an epimorphism $\phi : G \longrightarrow H$ fixing every $x \in X$ and such that Ker $\phi = \overline{S \setminus R}$. Conversely, every factor group of $G = \langle\, X \mid R \,\rangle$ has a presentation $\langle\, X \mid S \,\rangle$ with $R \subseteq S$.*

Proof. See [45]. □

We now present several fundamental results in the theory of group presentations that let us construct a procedure for showing that one presentation is isomorphic to another. If two presentations define the same group then they are said to be isomorphic - this is undecidable in general, see [58].

Lemma 1.10 *Let F, G and H be groups and $\nu : F \longrightarrow G$, $\alpha : F \longrightarrow H$ be homomorphisms such that*

$$(1) \quad \mathrm{Im}(\nu) = G,$$

$$(2) \quad \mathrm{Ker}(\nu) \subseteq \mathrm{Ker}(\alpha).$$

Then there is a homomorphism $\alpha' : G \longrightarrow H$ such that $\nu\alpha' = \alpha$.

Proof. See [45]. □

Lemma 1.11 (Substitution Test) *Let $G = \langle\ X \mid R\ \rangle$, H be a group and $\theta : X \longrightarrow H$ a mapping. Then θ extends to a homomorphism $\theta' : G \longrightarrow H$ if and only if, for all $x \in X$ and all $r \in R$, the result of substituting $x\theta$ for x in r yields the identity of H.*

Proof. See [45]. □

From these results we introduce the notion of Tietze transformations:

Lemma 1.12 *Let $F = F(X)$, $G = \langle\ X \mid R\ \rangle$ and suppose that $w, r \in F$ with w arbitrary and $r \in \overline{R} \setminus R$. If y is a symbol not in X, then both the "inclusions"*

$$X \longrightarrow \langle\ X \mid R, r\ \rangle$$

$$X \longrightarrow \langle\ X, y \mid R, y^{-1}w\ \rangle$$

extend to isomorphisms with domain G.

Proof. See [45]. □

The last result gives us four ways of manipulating a presentation, $\langle\ X \mid R\ \rangle$, to get $\langle\ X' \mid R'\ \rangle$, where both presentations define the same group. The possible

manipulations are called *Tietze transformations* and are defined as follows (from [45]) :

$R+$, adding a relator

$$X' = X,\ R' = R \cup \{r\}$$

where $r \in \overline{R} \setminus R$.

$R-$, removing a relator

$$X' = X,\ R' = R \setminus \{r\}$$

where $r \in R \cap \overline{R \setminus \{r\}}$.

$X+$, adding a generator

$$X' = X \cup \{y\}\ R' = R \cup \{y^{-1}w\}$$

where $y \notin X$ and $w \in F$.

$X-$, removing a generator

$$X' = X \setminus \{y\},\ R' = R \setminus \{y^{-1}w\}$$

where $y \in X$, $w \in \langle X \setminus \{y\} \rangle$ and $y^{-1}w$ is the only element of R involving y.

Two of the main areas in the study of finite group presentations are: given a group G find a presentation for it that satisfies certain requirements. The second approach is to obtain a presentation for a group construction given a presentation for the constituent groups. (This dual approach is, essentially, like that found in finite group theory as a whole, in that, in order to classify finite groups, one can find simple groups and then extensions of them.) It is from the latter area that we obtain the following, that will be of vital importance in subsequent chapters:

Lemma 1.13 *Let G be the finitely presented group with finite presentation $\langle X \mid R \rangle$ and let the group H be defined by the finite presentation $\langle Y \mid S \rangle$, where X and Y are disjoint sets. A presentation for the direct product of G and H, namely $G \times H$, is*

$$\langle X, Y \mid R, S, [X, Y] \rangle,$$

where $[X, Y] = \{x^{-1}y^{-1}xy \ : \ x \in X, y \in Y\}$.

Proof. See [45] or [62]. □

Another group we will be interested in is the group G/G', the group G factored out by its derived subgroup ($G' = \langle [x, y] \ : x, y \in G \rangle$). Fortunately there are two main ways to find information about this group.

A way of finding a presentation for G/G' given a presentation for G is:

Lemma 1.14 *Let the group G be defined by the finite presentation $\langle X \mid R \rangle$. A presentation for G/G' is*

$$\langle X \mid R, C \rangle,$$

where if $X = \{x_1, x_2, \ldots, x_n\}$ *then* $C = \{[x_i, x_j] \ : \ 1 \leq i < j \leq n\}$.

Proof. See [45]. □

Using this presentation we may use Tietze transformations to help us find $|G/G'|$ and more information.

The other standard way of finding information about G/G' when we are given a presentation for G is to use the relation matrix.

Definition 1.15 Let G be the group defined by the finite presentation

$$\mathcal{P} = \langle x_1, x_2, \ldots, x_n \mid r_1, r_2, \ldots, r_m \rangle.$$

The *relation matrix* of $\mathcal{P}$ is an $m \times n$ matrix where the entry b_{ij} is the sum of the exponents of the generator x_j in the relator r_i.

Example 1.16 Let G be the group defined by the presentation

$$\mathcal{P} = \langle\, x, y, z \mid x^3 = y^3, zxz^{-1} = y, (zx)^3 = 1, (zy)^2 = 1 \,\rangle.$$

The relation matrix of $\mathcal{P}$ is

$$\begin{pmatrix} 3 & -3 & 0 \\ 1 & -1 & 0 \\ 3 & 0 & 3 \\ 0 & 2 & 2 \end{pmatrix}.$$

Given an $m \times n$ relation matrix M we can perform specific row and column operations to reduce M to a matrix of the form $(D\ 0)$ or $\begin{pmatrix} D \\ 0 \end{pmatrix}$, where D is a diagonal matrix with $D = \text{diag}(d_1, d_2, \ldots, d_{\min(m,n)})$, $d_i \in \mathbb{N} \cup \{0\}$ and $d_i | d_{i+1}, 1 \leq i \leq \min(m, n)$. The operations we may apply to reduce our relation matrix to this standard form are:

(1) Interchange any two rows (columns).

(2) Add any integer multiple of one row (column) to another.

These operations are called *elementary row (column) operations.* The d_i's mentioned above are called *invariant factors of* $\mathcal{P}$.

Example 1.17 In our example above we have

$$\begin{pmatrix} 3 & -3 & 0 \\ 1 & -1 & 0 \\ 3 & 0 & 3 \\ 0 & 2 & 2 \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & 0 & 0 \\ 1 & -1 & 0 \\ 0 & 3 & 3 \\ 0 & 2 & 2 \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & 0 & 0 \\ 1 & -1 & 0 \\ 0 & 1 & 1 \\ 0 & 2 & 2 \end{pmatrix}$$

$$\longrightarrow \begin{pmatrix} 0 & 0 & 0 \\ 1 & -1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

$$\longrightarrow \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

So we have shown that $G/G' \cong C_1 \times C_1 \times C_\infty \cong C_\infty$, the infinite cyclic group.

Example 1.18 We now use the other 'standard' method to calculate G/G' where G is the group defined by the presentation

$$\langle\, x, y, z \mid x^3 = y^3, zxz^{-1} = y, (zx)^3 = 1, (zy)^2 = 1 \,\rangle.$$

First we form the presentation $\langle X \mid R,\ C \rangle$, where $C = [X, X] = \{\, [x, y] \ : \ x, y \in X\}$ as follows,

$$\langle\, x, y, z \mid x^3 = y^3, zxz^{-1} = y, (zx)^3 = 1, (zy)^2 = 1, [x, y] = 1, [x, z] = 1, [y, z] = 1 \,\rangle.$$

Now applying Tietze transformations we get:

$$\begin{aligned}
& \langle\, x, y, z \mid x^3 = y^3, zxz^{-1} = y, (zx)^3 = 1, (zy)^2 = 1, [x, y] = 1, [x, z] = 1, [y, z] = 1 \,\rangle, \\
\cong\ & \langle\, x, y, z \mid x^3 = y^3, x = y, z^3x^3 = 1, z^2y^2 = 1, [x, y] = 1, [x, z] = 1, [y, z] = 1 \,\rangle, \\
\cong\ & \langle\, x, y, z \mid x = y, zx = 1, [x, y] = 1, [x, z] = 1, [y, z] = 1 \,\rangle, \\
\cong\ & \langle\, x, y, z \mid x = y, z = x^{-1}, [x, y] = 1, [x, z] = 1, [y, z] = 1 \,\rangle, \\
\cong\ & \langle\, x, z \mid z = x^{-1}, [x, z] = 1 \,\rangle, \\
\cong\ & \langle\, z \mid \,\rangle, \\
\cong\ & C_\infty.
\end{aligned}$$

So we obtain the same result, as expected.

We now turn out attention to trying to find a 'smallest' presentation for a given group.

Definition 1.19 The *deficiency* of a finite group presentation $\langle\, X \mid R \,\rangle$, written $\mathrm{def}(\langle\, X \mid R \,\rangle)$, is the quantity $|R| - |X|$. The *deficiency of the finitely presented group* G, $\mathrm{def}(G)$, is the minimum of the deficiency over all finite presentations for G.

A natural question to ask is what is the minimum possible value of the deficiency of a finite group G? To answer this we will first need to introduce a group invariant called the Schur multiplier of the finite group G, written $M(G)$.

Definition 1.20 Let G be a finite group defined by the finite presentation $\langle\, X \mid R \,\rangle$. Let $F(X)$ be the free group on the set X and $\overline{R}$ be the normal closure of the set R in $F(X)$. The *Schur multiplier* of G, written $M(G)$, is defined as

$$M(G) \;=\; \frac{F(X)' \cap \overline{R}}{[F(X), \overline{R}]}$$

where $F(X)'$ is the derived subgroup of $F(X)$ i.e. the subgroup of $F(X)$ generated by all elements of the form $[x, y] = x^{-1}y^{-1}xy$ with $x, y \in F(X)$.

The above definition is due to Hopf, see [41].

We also take this opportunity to record the following:

Definition 1.21 Let G be a finite group. If a group H has a subgroup A such that

$$(1) \quad A \leq H' \cap Z(H),$$
$$(2) \quad H/A \cong G,$$
$$(3) \quad |A| = |M(G)|,$$

then H is called a *covering group of* G. If H satisfies just the first two conditions then H is a *stem extension of* G.

Remark 1.22 1. By the first condition above, the subgroup A is abelian.

2. The Schur multiplier may also be defined in terms of stem extensions. A *defining pair for* G, (H, A), is an ordered pair of groups such that the first two conditions in the above list hold. It can be shown that the orders of the first members H of defining pairs for G, are bounded. The subgroups A that are paired with the groups H of maximal order are all isomorphic to $M(G)$. Using the language of cohomology theory the Schur multiplier is the factor of the group of 2-cocycles by the group of 2-coboundaries; see [58] for a, relatively, clear description of these terms.

The following theorem justifies us taking the time to discuss the Schur multiplier.

Theorem 1.23 *If G is a finite group, then in any presentation using x generators, at least $x + d(M(G))$ relators are needed, where $d(M(G))$ is the minimum number of generators of $M(G)$ (also called the rank of $M(G)$, written rank$(M(G))$).*

The above theorem gives us information about a group G with the presentation $\langle X \mid R \rangle$ where $|R| < |X|$.

Corollary 1.24 *Let the group G be defined by the finite presentation $\mathcal{P} = \langle X \mid R \rangle$ with $|R| < |X|$ i.e. $\mathcal{P}$ has negative deficiency. Then G has infinite order.*

Proof. See [45] for a proof or alternatively use the relator matrix. □

Definition 1.25 A finite group G is called *efficient* if it has a presentation $\langle X \mid R \rangle$ where $|R| - |X| = d(M(G))$.

Showing that a group G is efficient is, in general, undecidable, as shown by bin Ahmad in [1].

Having an important group invariant like the Schur multiplier led people to find ways of calculating it. One such way is presented below, due to Johnson [45]:

Let the finite presentation $\langle X \mid R \rangle$ define the finite group G. Consider $H = \langle X \mid [X, R] \rangle$ where $[X, R] = \{ [x, r] : x \in X, r \in R \}$. Now the subgroup $N = \langle R \rangle$ is clearly central and abelian in H. Using the fundamental theorem of finitely generated abelian groups we may split N up into a torsion part (i.e. the elements of N of finite order) T and a torsion free subgroup TF (TF is free abelian), so that $N \cong T \times TF$. Using the Reidemeister-Schreier procedure we can find a presentation for N. Now we may use matrix methods to identify $M(G)$, as this is the torsion part of N.

Another practical method that can be used to calculate $M(G)$, based on rewriting systems, is presented in [51].

Knowing the Schur multipliers of the groups G and H it would be beneficial if we could use this information to calculate the multiplier of $G \times H$, $G \ltimes H$ (the semidirect product), etc.. Fortunately such a formula exists in the direct product

case, but before we see it we will need to introduce the tensor product of two groups.

Definition 1.26 Let A and B be two groups. The *tensor product* $A \otimes B$ is the group generated by the formal pairs $a \otimes b$, where $a \in A$ and $b \in B$, that satisfy

$$\begin{aligned}(a \otimes b_1)(a \otimes b_2) &= a \otimes (b_1 b_2) \\ (a_1 \otimes b)(a_2 \otimes b) &= (a_1 a_2) \otimes b\end{aligned}$$

It can be shown that $A \otimes B$ forms an abelian group isomorphic to $A/A' \otimes B/B'$, see [73]. It has also been shown that $A \otimes B$ is isomorphic to $[A, B]/[A, B, A * B]$, where $A * B$ is the free product of the groups A and B; again see [73].

We list below some more properties of the tensor product.

Lemma 1.27 *Let G and H be groups. Then the following are all true:*

$$\begin{aligned}G \otimes H &\cong H \otimes G, \\ G \otimes H &\cong G/G' \otimes H/H', \\ G \otimes (H \times K) &\cong (G \otimes H) \times (G \otimes K), \\ C_n \otimes C_m &\cong C_{(n,m)}.\end{aligned}$$

Proof. See [15] □

We can use the above results for the tensor product to calculate the Schur multiplier of the direct product of two finite groups using the following theorem.

Theorem 1.28 *Let A and B be two finite groups then*

$$M(A \times B) \cong M(A) \times M(B) \times (A \otimes B)$$

Proof. See [73]. □

The above formula is called the *Schur-Künneth formula* and will be used in several chapters of this thesis. It can obviously be used in an iterative manner as follows:

Example 1.29 The 'standard' presentation for the cyclic group of order 2, written C_2, is $\langle\, a \mid a^2 = 1 \,\rangle$ and so it has trivial Schur multiplier. Now

$$\begin{aligned} M(C_2 \times C_2) &\cong M(C_2) \times M(C_2) \times (C_2 \otimes C_2), \\ &\cong C_2 \end{aligned}$$

and so $C_2 \times C_2$ requires at least one more relator than the number of generators. In fact in this case the bound can be reached since $\langle\, a, b \mid a^2 = 1, b^2 = 1, [a,b] = 1 \,\rangle$ is a presentation defining $C_2 \times C_2$.

Now $M(C_2 \times C_2 \times C_2)$ can be calculated by

$$\begin{aligned} M(C_2 \times C_2 \times C_2) &\cong M(C_2^2 \times C_2), \\ &\cong M(C_2^2) \times M(C_2) \times (C_2^2 \otimes C_2), \\ &\cong C_2 \times (C_2 \otimes C_2) \times (C_2 \otimes C_2), \\ &\cong C_2 \times C_2 \times C_2. \end{aligned}$$

Thus $\mathrm{rank}(M(C_2^3)) = 3$ and an efficient presentation for C_2^3 on a minimal generating set is

$$\langle\, a, b, c \mid a^2 = 1, b^2 = 1, c^2 = 1, [a,b] = 1, [a,c] = 1, [b,c] = 1 \,\rangle.$$

Finally in this section we will be interested in the Todd-Coxeter coset enumeration procedure first described in [65]. Given a finite presentation defining a group G and a set of words, W, generating a subgroup H of G, the procedure returns $[G : H]$, if the index is finite. This procedure becomes an algorithm when

we restrict ourselves to examining only finite groups. The following texts explain the procedure from different view points; the traditional way of introducing the procedure is presented in [54]; in [62] we see the procedure reformulated in terms of automata theory, and finally in [60] we see the Todd-Coxeter coset enumeration procedure as a specific example of a more general procedure carried out on semigroups.

The heart of the procedure is the *coset table.* If we carry out a Todd-Coxeter enumeration on the finite group G using the normal subgroup $N \trianglelefteq G$ and if N satisfies certain requirements then we may read from the coset table, amongst other things, permutation generators for the group G/N; see [54] [58] and [62] for more information.

Most of the results in this thesis were suggested by results gained while carrying out machine implementations of the Todd-Coxeter procedure.

All computer calculations were carried out on a dual processor Athlon XP 1800+ (1.53GHz) machine with 3GB DDR 266 memory.

2 Definitions and results from number theory

We now define the well known Fibonacci numbers and the Lucas numbers:

Definition 2.1 The *Fibonacci numbers* are members of the sequence $(f_n)_{-\infty}^{\infty}$ defined by the recurrence relation $f_n = f_{n-2} + f_{n-1}$ for $n > 0$, $f_n = f_{n+2} - f_{n+1}$ if $n < 0$ and we 'seed' the sequence with $f_0 = 0$ and $f_1 = 1$. The *Lucas numbers* $(g_n)_{-\infty}^{\infty}$ are defined by an analogous recurrence relation but with 'seeds' $g_0 = 2$ and $g_1 = 1$.

There are many known results concerning Fibonacci and Lucas numbers; see [67] for an excellent review of the more classical results.

We will need the following result in a later chapter.

Lemma 2.2 *For the integer m, we have $f_m = f_5 f_{m-4} + f_4 f_{m-5}$.*

Proof. We use induction on m.

Starting with the base cases we get

$$m = 0 \qquad 0 = f_0 = f_5 f_{-4} + f_4 f_{-5} = 5(-3) + 3(5) = 0,$$
$$m = 1 \qquad 1 = f_1 = f_5 f_{-3} + f_4 f_{-4} = 5(2) + 3(-3) = 1.$$

Now assume the result holds for all values less than m. We have by the induction hypothesis, $f_{m-1} = f_5 f_{m-5} + f_4 f_{m-6}$ and $f_{m-2} = f_5 f_{m-6} + f_4 f_{m-7}$ so

$$f_m = f_{m-1} + f_{m-2} = f_5(f_{m-5} + f_{m-6}) + f_4(f_{m-6} + f_{m-7}) = f_5 f_{m-4} + f_4 f_{m-5}.$$

□

We will also introduce some standard number theory functions together with some examples, where appropriate, in order to elucidate the main ideas. Our first definition will be concerned with solving the equation $a \equiv x^2 \bmod p$ with $(a, p) = 1$. If a solution of the congruence $a \equiv x^2 \bmod p$ with $(a, p) = 1$ exists then a is said to be a *quadratic residue modulo p*; otherwise a is a *quadratic nonresidue modulo p*.

Definition 2.3 The *Legendre symbol* $(\frac{a}{p})$ is defined for all a which are not divisible by p; it is equal to 1 if there exists an x such that $a \equiv x^2 \bmod p$ with $(a, p) = 1$; otherwise it is equal to -1.

Much work has been carried out trying to understand this function; some of the results are listed below. More can be found in [69] together with the proofs of the following:

Theorem 2.4 *Let $p, p_1, p_2, \ldots, p_m$ be distinct odd prime numbers, $a_1, a_2, \ldots$ be numbers that are not divisible by $p, p_1, p_2, \ldots p_m$. Then*

$$\begin{aligned}
(\frac{a_1}{p}) &\equiv a_1^{(p-1)/2} \bmod p, \\
(\frac{a_1 a_2 \ldots a_n}{p}) &= (\frac{a_1}{p})(\frac{a_2}{p}) \ldots (\frac{a_n}{p}), \\
If\ a \equiv a_1 \bmod pp_1p_2 \ldots p_m \quad then \quad &(\frac{a}{pp_1p_2 \ldots p_m}) = (\frac{a_1}{pp_1p_2 \ldots p_m}), \\
(\frac{a_1 a_2^2}{p}) &= (\frac{a_1}{p}), \\
(\frac{p_1}{p}) &= (-1)^{(p-1)(p_1-1)/4}(\frac{p}{p_1}), \\
(\frac{a_1}{p_1 \ldots p_m}) &= (\frac{a_1}{p_1})(\frac{a_1}{p_2}) \ldots (\frac{a_1}{p_m}), \\
(\frac{2}{p}) &= (-1)^{(p^2-1)/8}, \\
(\frac{-1}{p}) &= (-1)^{(p-1)/2}.
\end{aligned}$$

Example 2.5 Can the congruence $x^2 \equiv 219 \bmod 383$ hold?

Using the above we get

$$\begin{aligned}
(\frac{219}{383}) &= -(\frac{383}{219}) = -(\frac{164}{219}) = -(\frac{2^2(41)}{219}) \\
&= -(\frac{41}{219}) = -(\frac{219}{41}) = -(\frac{14}{41}) \\
&= -(\frac{2}{41})(\frac{7}{41}) = -(-1^{(41^2-1)/8})(\frac{7}{41}) = -(\frac{7}{41}) \\
&= -(\frac{41}{7}) = -(\frac{6}{7}) = -(\frac{-1}{7}) \\
&= -(-1^{(7-1)/2}) = 1
\end{aligned}$$

Hence $x^2 \equiv 219 \bmod 383$ has a solution ($x = 169$ or $x = 383 - 169 = 214$ will do).

The notion of a primitive root will be of vital importance in later chapters of this thesis so we introduce:

Definition 2.6 A *primitive root in* $GF(p)$, where p is a prime number, is an element r of $GF(p)$ such that $\langle r \rangle = Z_{p-1}^*$, where Z_{p-1}^* is the multiplicative cyclic group of order $p-1$.

We will sometimes say that r is a primitive root mod p to mean that r is a primitive root in $GF(p)$.

Example 2.7 If $p = 11$ then the primitive roots of $GF(11)$ are $2, 6, 7$ and 8.

Before we give known results for primitive roots we will first need the following definition:

Definition 2.8 Let a, $a > 0$, be an integer. Then $\phi(a)$ is the number of integers in the range $[0, a-1]$ that are coprime to a. The symbol ϕ is called *Euler's function* or *Euler's Totient.*

From the definition it is obvious that if p is an odd prime $\phi(p) = p - 1$. Also if $p_1, p_2, \ldots, p_n$ are different prime numbers, $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$ and $\alpha_i \in \mathbb{N}$ then $\phi(a) = a(1 - 1/p_1)(1 - 1/p_2)\ldots(1 - 1/p_n)$; see any basic number theory text book, e.g. [69], for proofs of these standard results.

Related to Euler's function is the group theoretic idea of Hall's Eulerian function of a group.

Definition 2.9 Let G be a finitely generated group. We define *Hall's Eulerian function of the group* G, written $\phi_n(G)$, to be the number of n-tuples from G that can generate G.

Returning to primitive roots we have the following results:

Theorem 2.10 *Let r be a primitive root in $GF(p)$ where p is an odd prime. Then:*

(1) *There are $\phi(\phi(p)) = \phi(p-1)$ primitive roots in $GF(p)$.*

(2) *If $p = 4k+1$ is a prime such that $\phi(p-1)/(p-1) > 1/4$ and b is a quadratic residue modulo p, then there is at least one primitive root of p among the integers*

$$Z = \{g_1 + b, g_2 + b, \ldots, g_{\phi(p-1)} + b, g_1 + b', g_2 + b', \ldots, g_{\phi(p-1)} + b'\},$$

where g_i are the primitive roots of p, and b' denotes the solution of the congruence $bb' \equiv 1 \bmod p$.

(3) *If $p = 4k+3 > 3$ is a prime such that $\phi(p-1)/(p-1) > 1/3$ and b is an integer, $p \nmid b$, then there is at least one primitive root of p among the set Z.*

Proof. The first result is obvious while the other results are proved in [68]. □

There are several conjectures regarding primitive roots, for example:

Conjecture: For virtually all n, given arbitrary $\alpha, \beta \neq 0$ in $GF(n)$ there exists a primitive root r such that $\alpha r + \beta$ is also a primitive root in $GF(n)$. See [26] for more information about this conjecture.

We note here that we are using the phrase "virtually all" in the technical sense, i.e. for all but a finite number of exceptions.

Finally we will introduce the floor function.

Definition 2.11 The *floor* of a given real number x is the largest integer that is less than or equal to x. We denote the floor of x by $\lfloor x \rfloor$.

Chapter 2

Introduction to Fibonacci length and generalizations

1 Introduction and apology

In 1960 D. D. Wall investigated the length of the period of the Fibonacci numbers modulo a given positive integer n, see [71]. In his paper he introduced the Wall number symbol, $k(n)$, into the mathematical lexicon, defined as follows:

Definition 1.1 The minimal length of the period of the series $(f_i \bmod n)_{i=-\infty}^{\infty}$ is denoted by $k(n)$ and is called the *Wall number of* n.

Example 1.2 If $n = 5$ then the Wall number of 5 is 20, written $k(5) = 20$. To see this we use the table below:

n	1	2	3	4	5	6	7	8	9	10	11	12	13
$f_n \bmod 5$	1	1	2	3	0	3	3	1	4	0	4	4	3

n	14	15	16	17	18	19	20	21	22	23	24
$f_n \bmod 5$	2	0	2	2	4	1	0	1	1	2	...

A list of $k(p_i)$ for all primes p_i with $p_i < 1000$ is given in Appendix A.

In his paper Wall gave several interesting results:

Lemma 1.3 *If n and e are positive integers, $n > 2$, and p is a prime number then:*

(1) $k(n)$ is an even integer,

(2) $f_{k(n)+m} \equiv f_m \bmod n$, for any natural number m,

(3) $f_{mk(n)} \equiv 0 \bmod n$, for any natural number m,

(4) if $k(p^2) \neq k(p)$, then $k(p^e) = p^{e-1}k(p)$,

(5) if t is the largest integer with $k(p^t) = k(p)$, then $k(p^e) = p^{e-t}k(p)$ for $e > t$,

(6) if m has the prime factorization $m = \prod p_i^{e_i}$ and if $h_i = k(p_i^{e_i})$ then $k(m)$ is the lowest common multiple of the h_i,

(7) if $p = 10e \pm 1$, then $k(p)$ divides $p - 1$,

(8) if $p = 10e \pm 3$, then $k(p)$ divides $2p + 2$.

Proof. See [71]. □

Wall made a conjecture in [71] which is far deeper than it first appears:

Wall conjecture : For p a prime, $k(p^2) \neq k(p)$.

This conjecture can be reformulated as

Wall conjecture II : For p a prime, $p^2 | f_{p-(\frac{5}{p})}$ is always impossible, where (-) is the Legendre symbol; see [75].

Remark 1.4 It is known that $p | f_{p-(\frac{5}{p})}$ with $p \neq 5$; see [2] for proof. This result together with the proof of Theorem 5 from [71] shows that Wall's original conjecture implies Wall conjecture II.

This conjecture has been tested for all primes p where $p < 10^9$, see [75]. The non-triviality of the conjecture follows from work carried out by Sun and Sun, see [63]. They used the following definition:

Definition 1.5 Let p be an odd prime. If $x^p + y^p = z^p$ has no integer solution with $p \nmid xyz$ then we say that the *first case of Fermat's last theorem*, written (FLT1), holds for the exponent p, otherwise FLT1 fails for p.

In [63] it is shown that:

Theorem 1.6 *A positive answer to Wall's conjecture $\Longrightarrow$ FLT1 holds for all prime exponents.*

Proof. See [63]. □

It was not until 1986 that the ideas of Wall's paper were generalized to the area of group theory. In his paper H. J. Wilcox, see [74], placed Wall's results in the context of abelian groups and more specifically C_n. Some of Wilcox's results are:

Lemma 1.7 (1) *For $m > 2$, $k(m) = 2t$ where*

$$t = \min(\{n : \ n \text{ even and } m|f_n\} \cup \{n : \ n \text{ odd and } m|g_n\}),$$

(2) *any sequence of the form $a, b, ab, ab^2, \ldots, a^{f_{n-1}}b^{f_n}, \ldots$ in an abelian group G will have odd period > 3 only if it does not contain the identity element,*
(3) *a sequence of the form $a, a, a^2, \ldots, a^{f_n}, \ldots$ in a group G will have period $2n > 5$ if a has order f_n, for n even, or g_n, for n odd.*
Furthermore, to create a sequence of period $2n$ one could use an element a of order x, where x divides f_n for n even or g_n for n odd and x does not divide any previous f_n or g_n respectively.

Proof. See [74]. □

Then in 1990 C. M. Campbell, H. Doostie and E. F. Robertson, see [19], gave a natural generalization of Wilcox's work. This paper rigorously defined the notion of the Fibonacci orbit and Fibonacci length of a finite group G with respect to a generating set A of G (they restricted themselves to the case $|A| = 2$ but we will consider any finite generating set). Here we define the notion of Fibonacci orbit and length of a group G with respect to a finite generating set A.

Definition 1.8 Let G be a finitely generated group with generating set $A = \{a_1, a_2, \ldots, a_n\}$. Then the *Fibonacci orbit of G with respect to the (generating) set A*, where A is written as the ordered n-tuple $(a_1, a_2, \ldots, a_n)$, denoted by $F_A(G)$, is the sequence $x_0 = a_1, x_1 = a_2, \ldots, x_{n-1} = a_n$ and $x_{n+i} = \prod_{j=1}^{n} x_{i+j-1}, i \geq 0$.

It may be convenient to start the Fibonacci orbit from x_1 rather than x_0; in this case the orbit has the natural analogous definition.

In the subsequent chapters whenever the word set is used in conjunction with Fibonacci orbit or length we will mean ordered tuple, the reason for this will become apparent later on. The orbit is 'seeded' with n generators because of the following lemma that gives us a nice property of n consecutive members of the Fibonacci orbit:

Lemma 1.9 *Let G be a group generated by the set A. If $|A| = n$, then any n consecutive members of the Fibonacci orbit of G with respect to A is a generating set of G.*

Proof. The proof is a natural generalization of Lemma 2 in [19]. □

In some cases the Fibonacci orbit may form a repeating sequence in which case we can define:

Definition 1.10 If, for a group G and (generating) set A, $F_A(G)$ is periodic, then the minimal length of the period of the sequence is called the *Fibonacci length of G with respect to the (generating) set A*, written $LEN_A(G)$. When it is clear which (generating) set is being used we will write $LEN(G)$ for $LEN_A(G)$. If $F_A(G)$ is not periodic then G is said to have infinite Fibonacci length with respect to A.

Example 1.11 Wall's results are equivalent to finding the Fibonacci length of the cyclic group $C_n = \langle a \rangle$ using the generator a together with the identity element, so $k(n) = LEN_{(id,a)}(C_n)$.

Example 1.12 The dihedral groups, D_{2m}, of order $2m$ defined by the presentation $\langle\ a, b \mid a^2, b^m, (ab)^2\ \rangle$ have Fibonacci length 6. To see this we calculate the orbit

$$(a, b, ab, \underline{bab} = a, \underline{aba} = b^{-1}, ab^{-1}, \underline{b^{-1}ab^{-1}} = a, \underline{ab^{-1}a} = b, \ldots).$$

So $LEN_{(a,b)}(D_{2m}) = 6$.

All finite groups have finite Fibonacci length (since if $G = \langle X \rangle$, with $|X| = n$ then $LEN_X(G) \leq |G|^n$; this is a crude bound and will be sharpened later). Infinite groups may have finite or infinite Fibonacci length.

Example 1.13 Let $F(x, y)$ be the free group on the generators x and y. Then the Fibonacci orbit starts with

$$(x, y, xy, yxy, xy^2xy, yxyxy^2xy, xy^2xy^2xyxy^2xy, \ldots).$$

Obviously the orbit does not repeat and so the Fibonacci length is infinite. Each member of the Fibonacci orbit of $F(x, y)$ is a *Fibonacci word.* In this thesis we shall use the term Fibonacci word to mean the members of the Fibonacci orbit of the free group on two generators. A Fibonacci word is a word on two free

generators, x and y say, that follow the recurrence relation $x_1 = x, x_2 = y$ and $x_{i+2} = x_i x_{i+1}$ for $i \geq 1$. Fibonacci words can also be defined by the deterministic Lindenmayer system without interactions (DOL system)

$$\langle \{a, b\}, \{a \longrightarrow b, b \longrightarrow ab\}, a \rangle,$$

so we get $a, b, ab, (b)(ab), (ab)(b)(ab), (b)(ab)(ab)(b)(ab), \ldots$, see [59]. Combinatorial properties of Fibonacci words have been studied extensively e.g. see [50], [66] and [33].

In Example 1.12 the relation $b^m = 1$ is never used in the calculation of the orbit. Thus the infinite dihedral group D_∞ with presentation $\langle a, b | a^2 = 1, (ab)^2 = 1 \rangle$ has Fibonacci length 6.

Below we present a family of groups that, in certain circumstances, have finite Fibonacci length and in other circumstances have infinite Fibonacci length.

Lemma 1.14 *Let $G(l, x, y)$ be the group defined by the presentation*

$$\mathcal{B}(l, x, y) = \langle a, b \mid a^l \text{ and } b^2 \text{ are central}, a^x = b^y = 1 \rangle.$$

If $n \in \mathbb{N}$ then $LEN(G(2, hcf(f_{6n}, f_{6n-1} - 1), hcf(f_{6n}, f_{6n+1} - 1)) = 6n$. If $l = 3$ then $G(3, x, y)$ has infinite Fibonacci length.

Proof. Let y be an odd integer. We have $ab^y = b^y a$ but $y = 2r + 1$ so $ab^{2r+1} = b^{2r+1}a = bab^{2r}$ giving $ab = ba$ and the group is abelian and thus finite. So in this case the Fibonacci length of the group is finite.

So let y be a positive even integer. Using the notation of the lemma we calculate the Fibonacci orbit of $G(2, x, y)$.

$$\begin{aligned}(x_0 &= a, x_1 = b, x_2 = ab, x_3 = bab, x_4 = b(a^2b^2), x_5 = ba(a^2b^4),\\ x_6 &= a(a^4b^8), x_7 = b(a^8b^{12}), x_8 = ab(a^{12}b^{20}), x_9 = bab(a^{20}b^{32}),\\ &x_{10} = b(a^{34}b^{54}), x_{11} = ba(a^{54}b^{88}), \ldots).\end{aligned}$$

It is easy to see that for $n \geq 0$ the Fibonacci orbit of $G(2, x, y)$ can be split into segments of the form

$$\begin{aligned}(x_{6n} &= a(a^{f_{6n-1}-1}b^{f_{6n}}), x_{6n+1} = b(a^{f_{6n}}b^{f_{6n+1}-1}),\\ x_{6n+2} &= ab(a^{f_{6n+1}-1}b^{f_{6n+2}-1}), x_{6n+3} = bab(a^{f_{6n+2}-1}b^{f_{6n+3}-2}),\\ x_{6n+4} &= b(a^{f_{6n+3}}b^{f_{6n+4}-1}), x_{6n+5} = ba(a^{f_{6n+4}-1}b^{f_{6n+5}-1})).\end{aligned}$$

Thus if $|a| = hcf(f_{6n-1} - 1, f_{6n})$ and $|b| = hcf(f_{6n}, f_{6n+1} - 1)$ then $LEN(G(2, hcf(f_{6n}, f_{6n-1} - 1), hcf(f_{6n}, f_{6n+1} - 1)) = 6n$.

To see that $G(3, x, y)$ has infinite Fibonacci length we calculate the orbit. If $x_0 = a$ and $x_1 = b$ then $x_{10} = bababab(a^{18}b^{30})$ and $x_{11} = a^2babab(a^{30}b^{52})$. Now if we keep calculating the members of the orbit and 'moving' all occurrences of a^3 and b^2 to the right we will obtain entries of the form $x_m = babw_mbab(a^{3r}b^{2t})$, if m is even, and $x_m = a^2bw_mbab(a^{3r}b^{2t})$, if m is odd, where r and t are integers and $w_m \in \{a, b\}^*$. If m is even, $x_m = babw_mbab(a^{3r}b^{2t})$ and $x_{m+1} = a^2bw_{m+1}bab(a^{3u}b^{2v})$ where r, t, u, v are positive integers then:

$$\begin{aligned}x_{m+2} &= babw_mbaba^2bw_{m+1}bab(a^{3(r+u)}b^{2(t+v)}),\\ &= babw_{m+2}bab(a^{3(r+u)}b^{2(t+v)}),\\ x_{m+3} &= a^2bw_{m+1}babbabw_mbaba^2bw_{m+1}bab(a^{3(r+2u)}b^{2(t+2v)}),\\ &= a^2bw_{m+1}ba^2bw_mbaba^2bw_{m+1}bab(a^{3(r+2u)}b^{2(t+2v+1)}),\\ &= a^2bw_{m+3}bab(a^{3(r+2u)}b^{2(t+2v+1)}).\end{aligned}$$

It follows that as m increases so does the length of the w_m's and the number of occurrences of ab. Hence the orbit never repeats. □

Remark 1.15 We note that the previous argument would also be true if we used the groups $C_2 * C_2$ and $C_3 * C_2$ resp. (the free product of C_2 with itself, and the

free product of C_3 with C_2) with presentations

$$\langle\, a, b \mid a^2 = 1, b^2 = 1 \,\rangle,$$
$$\langle\, a, b \mid a^3 = 1, b^2 = 1 \,\rangle.$$

As a consequence of von Dyck's Lemma the groups $G(l, 2, 2)$ and $G(l, 3, 2)$ are epimorphic images of $C_2 * C_2$ and $C_3 * C_2$ resp.

The Fibonacci orbit and length of a group is a very finely balanced idea. For example the order in which the generators of a group are considered matters when calculating the Fibonacci length of a group as the following table illustrates:

n	3	4	5	6	7	8	9	10	11	12	13	14	15
$LEN_X(A_n)$	8	16	12	14	60	104	28	176	180	260	60	56	324
$LEN_Y(A_n)$	8	16	14	10	44	16	48	40	108	260	156	424	384

where $X = [(1, 2, 3, \ldots, n), (n{-}2, n{-}1, n)]$ and $Y = [(n{-}2, n{-}1, n), (1, 2, 3, \ldots, n)]$.

In the above A_n represents the alternating group on n symbols.

Remark 1.16 Thus in the definition of a Fibonacci orbit we need an ordered n-tuple, A, rather than a set.

It would be nice if one could give a general theory regarding the Fibonacci orbit or length of a group G. Unfortunately this has proved elusive in general. We do know that there is no simple formula that, given the Fibonacci length of a group G, can calculate the Fibonacci length of a subgroup. If $G \geq H$ or $G \trianglerighteq H$ any of the following are possible:

$$\begin{aligned} LEN(H) &\geq LEN(G), \\ LEN(H) &\leq LEN(G), \\ LEN(H) &\mid LEN(G), \\ LEN(H) &\nmid LEN(G). \end{aligned}$$

The following table gives examples of each of the above possible cases:

n	3	4	5	6	7	8	9	10	11	12	13	14	15
$LEN(S_n)$	6	18	54	216	42	150	432	900	252	720	720	252	300
$LEN(A_n)$	8	16	12	14	60	104	28	176	180	260	60	56	324

where $S_n = \langle (1,2,3,\ldots,n),(1,2)\rangle$ and $A_n = \langle (1,2,3,\ldots,n),(n-2,n-1,n)\rangle$ if n is odd and $A_n = \langle (1,2,3,\ldots,n-1),(n-2,n-1,n)\rangle$ if n is even.

We now look at the resulting Fibonacci length when one removes a generator of a group to obtain a subgroup.

Firstly the expected can happen i.e $LEN(\langle A\rangle) > LEN(\langle A \setminus a_i\rangle)$, where $a_i \in A$. An example of this is $LEN(\langle (1,2,3,4),(1,2),(5,6,7,8),(5,6)\rangle) = 90$ while $LEN(\langle (1,2,3,4),(1,2),((5,6,7,8)\rangle) = 24$.

To prove that the other inequality may hold, i.e $LEN(\langle A\rangle) < LEN(\langle A \setminus a_i\rangle)$ for $a_i \in A$, let

$$a = (1,13,4,16)(2,15,5,18)(3,14,6,17)(7,19,10,22)(8,21,11,24)(9,20,12,23),$$
$$b = (1,7)(2,8)(3,9)(4,10)(5,11)(6,12)(13,19)(14,20)(15,21)(16,22)(17,23)(18,24),$$
$$c = (1,2,3)(4,5,6)(7,8,9)(10,11,12)(13,14,15)(16,17,18)(19,20,21)(22,23,24).$$

The nonabelian group generated by a, b and c has order 24 with a proper normal subgroup generated by b and c of order 6. Then $LEN(\langle a,b,c\rangle) = LEN(\langle b,c,a\rangle) = 8$ but $LEN(\langle b,c\rangle) = 24$. So by this example we see that it is possible to have $LEN_A(\langle A\rangle) < LEN_{A\setminus a_i}(\langle A \setminus a_i\rangle)$, where $A = \{a_1, a_2, \ldots, a_n\}$ and $i \in \{1,2,3,\ldots,n\}$.

Another example of the above phenomenon is given by the dihedral groups, D_{2n}, defined by the presentation $\langle\ a,b \mid a^n, b^2, (ab)^2\ \rangle$. It has been shown that the Fibonacci length of D_{2n} given by this presentation is 6. Now $\langle a\rangle \lhd \langle a,b\rangle$ and $LEN(\langle a\rangle) = k(n)$ and so we need $6 < k(n)$ and we will have another example of

the above phenomenon; $n = 3$ will do since $k(3) = 8$.

Since we have given results concerning the Fibonacci orbit and length a natural question to ask is, why study this area? A reason for studying this area is that it gives information regarding the connections between the group being studied and a Fibonacci group. A Fibonacci group is defined by:

Definition 1.17 The *Fibonacci group* $F(r, n)$ is the group defined by the cyclic presentation

$$\langle a_1, a_2, \ldots, a_n \quad | \quad a_1a_2a_3 \ldots a_r = a_{r+1},\ a_2a_3a_4 \ldots a_{r+1} = a_{r+2},\ \ldots,$$
$$a_{n-1}a_na_1 \ldots a_{r-2} = a_{r-1},\ a_na_1a_2 \ldots a_{r-1} = a_r \rangle,$$

where $r > 0$, $n > 0$, and all subscripts are assumed to be reduced modulo n.

Fibonacci groups have been studied by many people. Typical questions that have been studied are trying to identify if $F(r, n)$ is finite or not, identifying $F(r, n)/F(r, n)'$, etc.; see [24], [46] and [64] for more information.

We now show the connection between the Fibonacci length of a group and a Fibonacci group.

Theorem 1.18 *Let G be a group with generating set $A = \{a_1, \ldots, a_n\}$ and let $LEN_A(G) = m$ for finite m. Then G is a epimorphic image of $F(n, m)$.*

Proof. This is a direct consequence of von Dyck's Lemma and [46]. □

Example 1.19 Let the dihedral group of order $2n$ be given as the finite presentation:

$$\langle\ a, b \mid a^2 = b^n = (ab)^2 = 1 \rangle.$$

So $F(2,6)$ has as an epimorphic image this family of groups. To see this we give the presentation of $F(2,6)$:

$$\langle\, a_1, a_2, \ldots, a_6 \mid a_3 = a_1a_2, a_4 = a_2a_3, a_5 = a_3a_4, a_6 = a_4a_5, a_1 = a_5a_6, a_2 = a_6a_1 \,\rangle$$

The group can obviously be generated by a_1 and a_2. To obtain a presentation for $F(2,6)$ on two generators we combine the relations given above as follows:

$$\begin{aligned}
a_3 &= a_1a_2, \\
a_4 &= a_2a_3 = a_2a_1a_2, \\
a_5 &= a_3a_4 = a_1a_2^2a_1a_2, \\
a_6 &= a_4a_5 = a_2a_1a_2a_1a_2^2a_1a_2, \\
a_1 &= a_5a_6 = a_1a_2^2a_1a_2^2a_1a_2a_1a_2^2a_1a_2, \\
a_2 &= a_6a_1 = a_2a_1a_2a_1a_2^2a_1a_2a_1.
\end{aligned}$$

Now a presentation for $F(2,6)$ is

$$\langle\, a_1, a_2 \mid a_1 = a_1a_2^2a_1a_2^2a_1a_2a_1a_2^2a_1a_2, a_2 = a_2a_1a_2a_1a_2^2a_1a_2a_1 \,\rangle.$$

In calculating the Fibonacci orbit of D_{2n} we have shown that $ab^2ab^2abab^2ab = a$ and $babab^2aba = b$ hold in the group, so D_{2n} has a presentation

$$\langle\, a, b \mid a^2 = b^n = (ab)^2 = 1, ab^2ab^2abab^2ab = a, babab^2aba = b \,\rangle.$$

The result follows from von Dyck's Lemma.

Having established that G is an epimorphic image of some Fibonacci group $F(r,n)$ we can use some results from general group theory to glean some information concerning $F(r,n)$, for example:

Theorem 1.20 *If $f : G \longrightarrow Q$ is a homomorphism, then*

(1) $f(G)^{(i)} = f(G^{(i)})$,

(2) $\gamma_i(f(G)) = f(\gamma_i(G))$,

(3) $[f(H), f(K)] = f([H,K])$ *for all subgroups H and K of G.*

Proof. See [62]. □

This result leads us to:

Corollary 1.21 *Let the Fibonacci length of G with respect to the generating set $A = \{a_1, a_2, \ldots, a_n\}$ be m, m finite. If G has nilpotency class c (resp. derived length i) then $f(\gamma_{c+1}(F(n,m))) \in \mathrm{Ker(f)}$ (resp. $f(F(n,m)^{(i)}) \in \mathrm{Ker(f)}$).*

Proof. Let G be as in the statement of the corollary. By Theorem 1.18 we know that there exists an epimorphism $f : F(n,m) \twoheadrightarrow G$. So by Theorem 1.20 we have $\gamma_{c+1}(f(F(n,m))) = \gamma_{c+1}(G) = \{\mathrm{id}\} = f(\gamma_{c+1}(F(n,m)))$.

The proof of the derived length statement follows from an analogous argument. □

There are still many open questions about Fibonacci lengths and orbits.

Open questions: Let G and H be groups.

1. Let X and Y generating sets of G. Can $LEN_X(G)$ be finite while $LEN_Y(G)$ is infinite?
2. Does knowing about the Fibonacci orbit of G and H give us information about the orbit, or length, of $G \times H$?
3. Let G be an extension of K by Q. If we know the Fibonacci orbit or length of G what can we say about the orbit or length of Q, or K?

2 Generalizations

We note here that there are many possible generalizations of the idea of Fibonacci length and orbit. Some work has been carried out on generalizing the recurrence

relation that one uses, see [57]. Ideas related to the Fibonacci length but carried out in finite semigroups, rather than groups, have been shown to be related to regularity preserving functions in automata theory, see [76].

Below we introduce two sections that investigate two generalizations of the Fibonacci length.

2.1 Maximum lengths

There are several possible generalizations of the definition for Fibonacci length. Below we define a special type of Fibonacci orbit of cyclic p-groups:

Definition 2.1 Let $G = \langle a \rangle$ be a cyclic group of order p^n, p a prime. A Fibonacci orbit of G with respects to the generating set $\{id, a\}$ will be said to be *maximal* if the orbit contains $p^n - 1$ elements.

We start by saying when an orbit will not be maximal.

Lemma 2.2 *Let p be a prime and n an integer, $n \geq 1$. If $x \in \{0, 1, 2, \ldots, p^n - 1\}$ is not in the sequence $(f_i \bmod p^n)_{i=0}^{\infty}$ then x will not be in the sequence $(f_i \bmod p^{n+1})_{i=0}^{\infty}$.*

Proof. Let x not appear in the sequence $(f_i \bmod p^n)_{i=0}^{\infty}$. Then $x \not\equiv f_{m-1} \bmod p^n + f_{m-2} \bmod p^n$. Now every entry in the sequence $(f_i \bmod p^{n+1})_{i=0}^{\infty}$ is of the form $z + hp^n$ where $z \in (f_i \bmod p^n)_{i=0}^{\infty}$ and $h \in \{0, 1, \ldots, p-1\}$. If $x \in (f_i \bmod p^{n+1})_{i=0}^{\infty}$ then it can be written in the following form: $x = z_1 + h_1 p^n + z_2 + h_1 p^n$. But $0 \leq x < p^n$, so $x = z_1 + z_2$ a contradiction and hence the result. □

We now use this result to find all maximal orbits of C_{p^n}.

Lemma 2.3 *Let $p = 2$. When $n = 1$ or 2 the sequence $(f_i \bmod p^n)_{i=0}^{\infty}$ is maximal and when $n \geq 3$ the sequence is not maximal.*

Proof. Using direct calculation we see that:

$$\begin{aligned} n &= 1 \quad (0,1,1,0,1,\ldots), \\ n &= 2 \quad (0,1,1,2,3,1,0,1,\ldots), \\ n &= 3 \quad (0,1,1,2,3,5,0,5,5,2,7,1,0,1,\ldots). \end{aligned}$$

From the last lemma the result holds. □

Having dealt with the prime 2 we now proceed to the prime 5.

Definition 2.4 Let $A = (a_n)_{n=1}^{\infty}$ be an infinite sequence of integers. For integers r and m, $m \geq 2$, let $A(N, r, m)$ denote the number of terms of a_n such that $n \leq N$ and $a_n \equiv r \bmod m$. If

$$\lim_{N \longrightarrow \infty} \frac{A(N,r,m)}{N} = \frac{1}{m}$$

for $r = 0, 1, \ldots, m-1$ then the sequence A is *uniformly distributed* modulo m.

Lemma 2.5 *The Fibonacci numbers are not uniformly distributed modulo p for any prime $p > 2$ and $p \neq 5$. Also (f_i) is uniformly distributed modulo 5^i for $i = 1, 2, \ldots$.*

Proof. See [53]. □

We now use a result from Wall's original paper to eliminate a large number of primes.

Lemma 2.6 *If p is a prime of the form $10x \pm 1$ then $k(p)|(p-1)$.*

Proof. See [71]. □

From this result we immediately deduce:

Corollary 2.7 *If p is a prime of the form $10x \pm 1$ then C_p does not have a maximal Fibonacci orbit.*

So we are left with primes of the form $10x \pm 3$. These will fall into several categories.

Lemma 2.8 *The Fibonacci orbit of C_3 and C_7 are maximal, but C_{3^2} and C_{7^2} do not yield maximal orbits.*

Proof. Let us examine C_j. The results follow by direct calculation and the use of Lemma 2.2 as follows:

$j = 3$ $(0, 1, 1, 2, 0, 2, 2, 1, 0, 1, \ldots)$,

$j = 3^2$ $(0, 1, 1, 2, 3, 5, 8, 4, 3, 7, 1, 8, 0, 1, \ldots)$,

$j = 7$ $(0, 1, 1, 2, 3, 5, 1, 6, 0, 6, 6, 5, 4, 2, 6, 1, 0, 1, \ldots)$,

$j = 7^2$ $(0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 6, 40, 46, 37, 34, 22, 7, 29, 36, 16, 3, 19, 22, 41,$
$14, 6, 20, 26, 46, 23, 20, 43, 14, 8, 22, 30, 3, 33, 36, 20, 7, 27, 34, 12, 46, 9, 6,$
$15, 21, 36, 8, 44, 3, 47, 1, 48, 0, 48, 48, 47, 46, 44, 41, 36, 28, 15, 43, 9, 3, 12,$
$15, 27, 42, 20, 13, 33, 46, 30, 27, 8, 35, 43, 29, 23, 3, 26, 29, 6, 35, 41, 27, 19,$
$46, 16, 13, 29, 42, 22, 15, 37, 3, 40, 43, 34, 28, 13, 41, 5, 46, 2, 48, 1, 0, 1, \ldots)$.

When $j = 7^2$ the numbers $4, 10, 11, 17, 18, 24, 25, 31, 32, 38, 39$ and 45 are missing. □

Before we deal with the remaining primes we illustrate a property of the Fibonacci sequence when it is considered modulo p, where p is a prime of the form $10x \pm 3$, for $x \geq 1$, and $p > 7$.

Let $p = 13$ then $k(13) = 28$:

n	1	2	3	4	5	6	**7**	8	9	10	11	12	13	**14**	15	16
$f_n \bmod 13$	1	1	2	3	5	8	**0**	8	8	3	11	1	12	**0**	12	12

n	17	18	19	20	**21**	22	23	24	25	26	27	**28**	29	30
$f_n \bmod 13$	11	10	8	5	**0**	5	5	10	2	12	1	**0**	1	...

Now let $p = 23$:

n	1	2	3	4	5	6	7	8	9	10	11	**12**	13	14	15	16
$f_n \bmod 23$	1	1	2	3	5	8	13	21	11	9	20	**6**	3	9	12	21
$f_n f_{n-5}^{-1} \bmod 23$	15	12	21	3	-	8	13	22	19	11	14	4	10	5	9	16

n	17	18	19	20	21	22	23	**24**	25	26	27	28	29	30
$f_n \bmod 23$	10	8	18	3	21	1	22	**0**	22	22	21	20	18	15
$f_n f_{n-5}^{-1} \bmod 23$	17	18	2	6	1	7	20	0	15	12	21	3	-	8

n	31	32	33	34	35	**36**	37	38	39	40	41	42	43	44
$f_n \bmod 23$	10	2	12	14	3	**17**	20	14	11	2	13	15	5	20
$f_n f_{n-5}^{-1} \bmod 23$	13	22	19	11	14	4	10	5	9	16	17	18	2	6

n	45	46	47	**48**	49	50
$f_n \bmod 23$	2	22	1	**0**	1	1
$f_n f_{n-5}^{-1} \bmod 23$	1	7	20	0	15	12

The important pattern in the above sequences is that at $n = p + 1$ we have $f_{n+k} \equiv (-1)^{k+1} f_{n-k} \bmod p$, for $k \in \mathbb{Z}$. This is an 'almost symmetric' property. This property induces a related effect at the points $n = (p + 1)/2$ and $n = 3(p+1)/2$, because $f_1 = 1 \equiv -f_p \bmod p$ and $p+1$ is even, where $f_{n+k} \equiv (-1)^k f_{n-k} \bmod p$.

Also note that $f_{p+1} \equiv 0 \bmod p$ and that $f_n f_{n-5}^{-1} \bmod 23$, where n runs over 23 consecutive numbers, are all different (although some of them are not defined).

Lemma 2.9 *If p is a prime of the form $10x \pm 3$, $p > 7$, then C_p does not have a maximal Fibonacci orbit.*

Proof. Let p be a prime of the form $10x \pm 3$, $p > 7$, and let all congruences be modulo p.

It is shown in [71] that if $p = 10x \pm 3$ then $f_p \equiv -1$, $f_{p+1} \equiv 0$, $f_{p+a} \equiv -f_{(p+a)-(p+1)}$ and $k(p)|(2p+2)$. Assume that $LEN(C_p) = 2(p+1)$. From $f_{p+1} \equiv 0$ and $f_p \equiv -1$ we get $f_{p-1} \equiv 1, f_{p-2} \equiv -2, \ldots, f_{(p+1)-m} \equiv (-1)^{m+1} f_{(p+1)+m} \equiv (-1)^m f_m$. So we have the 'almost symmetric' property pointed out above.

We have two possibilities for $f_{(p+1)/2}$:

- $f_{(p+1)/2} \equiv 0$

We examine the terms $f_0 \equiv 0, f_1 \equiv 1, \ldots, f_{(p+1)/2} \equiv 0$. This is a collection of $\frac{p+1}{2} + 1$ numbers, but $f_0 \equiv f_{(p+1)/2} \equiv 0$ and $f_1 \equiv f_2 \equiv 1$ so there are at least $\frac{p+1}{2} + 1 - 2 = \frac{p-1}{2}$ different numbers in the collection. By the 'almost symmetric' property the other entries of the Fibonacci orbit can only be numbers from the collection or their negative values. Thus there are, at most, $p-1$ different numbers in the Fibonacci orbit. In this case C_p does not have a maximal Fibonacci orbit.

- $f_{(p+1)/2} \equiv m$, $m \neq 0$

Again we examine the collection, $f_0 \equiv 0, f_1 \equiv 1, \ldots, f_{(p+1)/2} \equiv m$. This time we can only say that $f_1 = f_2 = 1$ and so the collection contains, at most, $\frac{p+1}{2} + 1 - 1 = \frac{p+1}{2}$ different numbers.

Now we show that, for two different entries of the collection, we have

$$f_a \equiv \pm f_b$$

for some a, b where $1 \leq a < b \leq (p+1)/2$. Showing this, together with the 'almost symmetric' property of the sequence, means that the orbit cannot contain every member of the set $\{0, 1, 2, \ldots, p-1\}$ and so C_p will not have a maximal Fibonacci orbit.

First note that $f_m f_{m-5}^{-1}$, $m \in \{5, 6, \ldots, p+4\}$ are all different. We prove this by contradiction. Assume that for $n \neq m$, where $n, m \in \{5, 6, \ldots, p+4\}$, we have $f_m f_{m-5}^{-1} \equiv f_n f_{n-5}^{-1}$. By writing $f_m = f_5 f_{m-4} + f_4 f_{m-5}$ we get

$$\begin{aligned}(f_5 f_{m-4} + f_4 f_{m-5}) f_{m-5}^{-1} &\equiv (f_5 f_{n-4} + f_4 f_{n-5}) f_{n-5}^{-1} \\ f_5 f_{m-4} f_{m-5}^{-1} + f_4 &\equiv f_5 f_{n-4} f_{n-5}^{-1} + f_4 \\ f_{m-4} f_{n-5} &\equiv f_{n-4} f_{m-5}.\end{aligned}$$

More generally this gives

$$f_{m-i-4} f_{n-i-5} \equiv f_{n-i-4} f_{m-i-5}.$$

Put $i = m - 6$ in the above to give $f_2 f_{n-m+1} \equiv f_{n-m+2} f_1$, that is, $f_{n-m+1} \equiv f_{n-m+2}$. By using the recurrence relation of the Fibonacci numbers we obtain $f_{n-m} \equiv 0$ but $m \geq 5$ so we must have $n = m$, a contradiction to the assumption. So the values of $f_m f_{m-5}^{-1}$, $m \in \{5, 6, \ldots, p+4\}$, are all different.

So for a certain m , $5 \leq m \leq p+4$ we have $f_m \equiv f_{m-5}$. To finish the proof we examine the four possible cases for the value of m.

- $m \geq p$

In this case we use the 'almost symmetric' property about the point f_{p+1} and then again about the point $f_{(p+1)/2}$ to get $f_a \equiv \pm f_b$ for some $1 \leq a, b \leq (p+1)/2$, and the result follows from this.

- $p > m > m - 5 > (p-1)/2$

By the 'almost symmetric' property of the sequence we have $f_m \equiv f_{m-5}$ for $1 \leq m \leq (p+1)/2$, the desired result.

- $m > (p-1)/2 > m - 5$

Let $m = (p-1)/2 + r$ where $1 \leq r \leq 4$. We have

$$\begin{aligned}f_{(p-1)/2+r} &\equiv f_{(p-1)/2-(5-r)} \text{ since } f_m \equiv f_{m-5}, \\ f_{(p-1)/2+r} &\equiv \pm f_{(p-1)/2-r} \text{ by the 'almost symmetric' property,}\end{aligned}$$

hence

$$f_{(p-1)/2-(5-r)} \equiv \pm f_{(p-1)/2-r}.$$

So we have two Fibonacci numbers of the form $f_a \equiv \pm f_b$, for $1 \leq a < b \leq (p+1)/2$, and so the result holds in this case.

- $(p-1)/1 \geq m$

This gives $f_m \equiv f_{m-5}$ for $1 \leq m \leq (p+1)/2$, the desired result. □

We now turn our attention to looking at nonabelian groups. To do this we will need to alter our definition of a maximal Fibonacci orbit, but first we will need some more definitions.

Definition 2.10 If G is a group, then its *Frattini subgroup* $\Phi(G)$ is defined as the intersection of all the maximal subgroups of G.

Definition 2.11 An element $x \in G$ is called a *nongenerator* if it can be omitted from any generating set: if $G = \langle x, Y \rangle$ then $G = \langle Y \rangle$.

We now give some well known results concerning the Frattini subgroup.

Theorem 2.12 *Let G be a group.*

(1) *The Frattini subgroup $\Phi(G)$ is the set of all nongenerators of G.*

(2) $G' \cap Z(G) \leq \Phi(G)$.

(3) *If G is finite then $\Phi(G)$ is nilpotent.*

(4) *A finite group G is nilpotent if and only if $G' \leq \Phi(G)$.*

Proof. See [58]. □

So, given a finite group G, we have the bound: $LEN_X(G) \leq |G \setminus \Phi(G)|^{|X|}$.

Definition 2.13 Let G be a nonabelian group and let X be a generating set for G. Then a Fibonacci orbit with respect to X is said to be *maximal* if it contains $|G \setminus \Phi(G)|$ different elements.

Note: In this section we will deal with minimal generating sets X, i.e. X is a *minimal generating set* for G if $G = \langle X \rangle$ and $Y \subset X$ then $\langle Y \rangle \neq G$. If we relax this condition we obtain a definition that is equivalent to a k-nacci sequence, see the next section for definitions and results concerning k-nacci sequences.

Such maximal orbits do exist, but not always, as the following examples illustrate.

Example 2.14 The dihedral group of order six, written $D_{2(3)}$, can be defined by the presentation $\langle a, b \mid a^2, b^2, (ab)^3 \rangle$. The Fibonacci orbit of this is easily seen to be $(a, b, ab, bab, b, ba, a, b, \ldots)$. Now $\Phi(D_{2(3)}) = \{ \text{ id } \}$. So the Fibonacci orbit given is maximal. In fact, by the results in [19], all Fibonacci orbits of $D_{2(3)}$ will be maximal.

Example 2.15 The generalized quaternion group Q_{2^n}, $n \geq 3$, can be presented by:

$$\langle a, b \mid a^{2^{n-1}} = 1, b^2 = a^{2^{n-2}}, b^{-1}ab = a^{-1} \rangle.$$

It is known that $\Phi(Q_{2^n}) = \langle a^2 \rangle$ and so $|\Phi(Q_{2^n})| = a^{2^{n-2}}$. From [19] the Fibonacci orbit of Q_{2^n} is seen to be $(a, b, ab, a^{2^{n-2}-1}, a^{2^{n-2}+2}b, ab, a, b, \ldots)$. Thus Q_{2^n} does not have a maximal Fibonacci orbit on that generating set.

One of the main barriers to studying maximal Fibonacci orbits is the lack of efficient algorithms that can calculate the Frattini subgroup of a given group. Methods exist to calculate the Frattini subgroup if the group is given as a finite group or a polycylically presented group. The result is also known if the group is simple, the Frattini subgroup is trivial in this case.

To overcome this problem we turn our attention to the study of p-groups. This area of group theory has some nice results concerning the Frattini subgroup. Also, by the Burnside Basis Theorem i.e. if G is a finite p-group, then any two minimal generating sets have the same cardinality, namely dim $G/\Phi(G)$. Moreover, every $x \notin \Phi(G)$ belongs to some minimal generating set of G, see [58], the notion of a minimal generating set and a generating set of minimal cardinality coincide (in general this is not true e.g. if $C_2 = \langle a \rangle$ and $C_3 = \langle b \rangle$ then $C_2 \times C_3$ has minimal generating set $\{a, b\}$ but $\{ab\}$ is a generating set of smallest cardinality).

Theorem 2.16 *Let G be a p-group. Then*

(1) $\Phi(G) = G'G^p$.

(2) *$G/\Phi(G)$ is a vector space over $\mathbb{Z}_p$.*

Proof. See [58]. □

The class of p-groups is huge so we restrict ourselves to the study of a subclass of them, namely the extra-special p-groups.

Definition 2.17 A finite p-group G is called *extra-special* if $Z(G) = G'$ and $|Z(G)| = p$.

This gives:

Lemma 2.18 *If G is an extra-special p-group then $\Phi(G) = G'$.*

Proof. Write $Z(G) = G' = \langle x \rangle$. Let $g, h \in G$ then $[h, g^p] = [h, g]^p$. Now $[h, g] \in G'$ and since $|G'| = p$, $[h, g]^p = 1$. Thus $[h, g^p] = 1$, so $G^p \leq Z(G)$ giving $\Phi(G) = G'G^p = G'$. □

So we have $|G \setminus \Phi(G)| = |G \setminus G'G^p| = |G \setminus G'| = p^n - p$. It is well known that every nonabelian group of order p^3, for p a prime, is extra-special. In fact we know:

Theorem 2.19 *Let G be a nonabelian group of order p^3, where p is an odd prime. Then G is extra-special and is isomorphic to the group defined by one of the following presentations:*

$$\langle\, x, y \;\mid\; x^p = 1, y^p = 1, [x,y]^x = [x,y] = [x,y]^y \,\rangle,$$
$$\langle\, x, y \;\mid\; x^{p^2} = 1, y^p = 1, x^y = x^{1+p} \,\rangle.$$

The groups defined by these presentations have exponent p and p^2 respectively. If $p = 2$ then $G \cong D_{2(4)}$ or Q_8.

Proof. See [56]. □

So to see if an extra-special p-group of order p^3 has a maximal Fibonacci orbit we first need to calculate its Fibonacci length.

Lemma 2.20 *Let p be an odd prime. The group defined by the presentation*

$$\mathcal{P}_p = \langle\, x, y \;\mid\; x^{p^2} = 1, y^p = 1, x^y = x^{1+p} \,\rangle$$

is isomorphic to the group defined by the presentation

$$\mathcal{F}_p = \langle\, a, b \;\mid\; ab = b^{p+1}a, ba = a^{p+1}b \,\rangle.$$

Proof. The proof follows once we have the results of Theorem 2.19. In [21] it is shown that the group defined by the presentation

$$\mathcal{H}(n,\ell) = \langle\, a, b \;\mid\; ab^n = b^\ell a, ba^n = a^\ell b \,\rangle$$

has order $|\ell - n|^3$ and the generators have order $(n-\ell)^2$. So the presentation $\mathcal{H}(1, p+1)$ defines a nonabelian group of order p^3 whose generators have order p^2 and so is isomorphic to the group defined by $\mathcal{P}_p$ by Theorem 2.19. □

So this leads to:

Corollary 2.21 *Let G be a nonabelian group of order p^3, where p is an odd prime. Then G is isomorphic to the group defined by one of the following presentations:*

$$\langle\, x, y \;\mid\; x^p = 1, y^p = 1, [x,y]^x = [x,y] = [x,y]^y \,\rangle,$$
$$\langle\, x, y \;\mid\; xy = y^{p+1}x, yx = x^{p+1}y \,\rangle.$$

The groups defined by these presentations have exponent p and p^2 respectively. If $p = 2$ then $G \cong D_{2(4)}$ or Q_8.

Now a final theorem we will need is:

Theorem 2.22 *Let $p > 3$ be a prime number. Then, if G is a nontrivial finite p-group of exponent p and nilpotency class 2, $LEN(G) = k(p)$.*

Proof. See [3]. □

Having this result we can say if the above groups have maximal Fibonacci orbits.

Theorem 2.23 *Let p be an odd prime. The groups of order p^3 defined by the presentations*

$$\mathcal{D}_p = \langle\, x, y \;\mid\; x^p = 1, y^p = 1, [x,y]^x = [x,y] = [x,y]^y \,\rangle,$$
$$\mathcal{F}_p = \langle\, x, y \;\mid\; xy = y^{p+1}x, yx = x^{p+1}y \,\rangle.$$

do not have maximal Fibonacci orbit. If $p = 2$ then $G \cong D_{2(4)}$ or Q_8 and these groups do not have maximal Fibonacci orbit.

Proof. We first deal with the case $p = 2$. By Lemma 2.19 and the definition of an extra-special p-group we know that $|\Phi(D_{2(4)})| = 2$ and $|\Phi(Q_8)| = 2$. By results of [19] we know that $LEN(D_{2(4)}) = 6$ and $LEN(Q_8) = 3$, and the Fibonacci

orbit of $D_{2(4)}$ contains 5 different elements while the orbit of Q_8 has 3 distinct elements. Thus neither $D_{2(4)}$ nor Q_8 have maximal Fibonacci orbits.

Let p be an odd prime. We consider each presentation separately:

- $\mathcal{D}_p$.

Firstly let $p > 3$. Then by Theorem 2.19 we see that the group D_p defined by $\mathcal{D}_p$ has exponent p. Since D_p is extra-special we have $[D_p', D_p] = [Z(D_p), D_p] = 1$ and so D_p has class 2. We also know that $|D_p - \Phi(D_p)| = p^3 - p$. So we have $LEN(D_p) = k(p) \leq (p^2 - 1) < p^3 - p$ and so D_p cannot have a maximal Fibonacci orbit.

If $p = 3$ we have $|D_3 - \Phi(D_3)| = 24$ and $LEN(D_3) = k(3) = 8$. So D_3 does not have maximal Fibonacci orbit.

- $\mathcal{F}_p$.

Let the group defined by $\mathcal{F}_p$ be F_p. By a result from Chapter 3 we have $LEN(F_p) = k(p^2)$; see Theorem 3.16 from Chapter 3 for further information and proofs. Now, for any prime p, either $k(p^2) = k(p)$ or $k(p^2) = pk(p)$, so we have one of the following:

$$(1) \quad LEN(F_p) = k(p^2) = k(p) \leq (p^2 - 1) < p^3 - p = |F_p - \Phi(F_p)|,$$

$$(2) \quad LEN(F_p) = k(p^2) = pk(p) \leq p(p^2 - 1) \leq p^3 - p = |F_p - \Phi(F_p)|.$$

We may have equality in (2) but by a result in [67] we have $k(p) = p^2 - 1$ for $p = 2$ or 3 only. The case $p = 2$ has already been dealt with. If $p = 3$ then $LEN(F_3) = k(9) = 24 = |F_3 - \Phi(F_3)|$ so in this case we may have a maximal orbit. A simple calculation shows that the Fibonacci orbit of F_3 has 20 distinct elements and so F_3 does not have a maximal orbit. □

Finally for this section we shall look at p-groups that have a single subgroup of order p. Such groups are classified in the following theorem:

Theorem 2.24 *A finite p-group has exactly one subgroup of order p if and only if it is cyclic or a generalized quaternion group.*

Proof. See [56]. □

Having dealt with cyclic groups of prime power order we concentrate on non-abelian groups with a single subgroup of order p.

Theorem 2.25 *If G is a noncyclic p-group with a single subgroup of order p then G does not have a maximal Fibonacci orbit.*

Proof. The case $n = 3$ has already been dealt with. Let G be a generalized quaternion group. So $|G| = 2^n$ for some n, $n > 3$. By Theorem 2.24 we need only examine generalized quaternion groups. Using the result of [19] we have $LEN(G) = 6$ for any generating pair. From Example 2.15 we have $|\Phi(G)| = 2^{n-1}$. So putting all this together we have:

$$LEN(G) = 6 < 2^{n-1} = 2^n - 2^{n-1} = |G \setminus \Phi(G)|$$

since $n > 3$. □

Open question : Another family of groups that would be interesting to investigate are the elementary groups (these are defined as groups G with $\Phi(H) = \{ \text{id} \}$ for each subgroup $H \leq G$); see [9] and [10] for more information.

2.2 k-nacci sequences

In this section we concentrate on a generalization of a maximal Fibonacci orbit first presented in [48] by S. W. Knox.

Definition 2.26 Let $j \leq k$. A *k-nacci sequence* in a finite group G is a sequence of elements of G for which, given an initial (ordered) *seed set* $x_0, x_1, \ldots, x_{j-1}$, the

remaining elements of the sequence are calculated using the following recurrence relation

$$x_n = \begin{cases} x_0 x_1 \dots x_{n-1} \text{ for } j \leq n < k \\ x_{n-k} x_{n-k+1} \dots x_{n-1} \text{ for } n \geq k \end{cases}$$

We also require that the elements $x_0, x_1, \dots, x_{j-1}$ generate G.

The k-nacci sequence of G with seed set $x_0, x_1, \dots, x_{j-1}$ is denoted by $F_k(G; x_0, x_1, \dots, x_{j-1})$. It is easy to see that this sequence repeats in a finite group.

Remark 2.27 It is easy to see that $F_k(G; x_0, x_1, \dots, x_{j-1})$ is the Fibonacci orbit of G with respect to the generating set $\{x_0, x_1, \dots, x_{j-1}, x_j = x_0 x_1 \dots x_{j-1}, x_{j+1} = x_0 x_1 \dots x_{j-1} x_j, \dots, x_{k-1} = x_0 x_1 \dots x_{k-1} x_{k-2}\}$. For example $F_4(G; x_0, x_1)$ is the sequence

$$\begin{aligned} (\quad & x_0, x_1, x_2 = x_0 x_1, x_3 = x_0 x_1 x_2 = x_0 x_1 x_0 x_1, \\ & x_4 = x_0 x_1 x_2 x_3, x_5 = x_1 x_2 x_3 x_4, x_6 = x_2 x_3 x_4 x_5, \dots), \end{aligned}$$

which is the Fibonacci orbit of G with respect to $\{x_0, x_1, x_2, x_3\}$.

Definition 2.28 A group G is *k-nacci sequenceable* if there exists a k-nacci sequence in which every element of the group is present.

Remark 2.29 With Remark 2.27 in mind we see that G is k-nacci sequenceable on an (ordered) seed set $x_0, x_1, \dots, x_{j-1}$ if and only if G has a maximal Fibonacci orbit with respect to the (ordered) set $x_0, x_1, \dots, x_{j-1}, x_n = x_0 x_1 \dots x_{n-1}$ where $j \leq n \leq k$.

At the end of [48] the following open question was posed:

Are all nonsimple k-nacci sequenceable groups nontrivial extensions of a k-nacci sequenceable group by a k-nacci sequenceable group? That is, does a nonsimple k-nacci sequenceable group have a k-nacci sequenceable normal subgroup?

In this section we intend to answer this question in general and thus complete the following table

	$N \lhd G$, N *is* *k-nacci sequenceable*	$N \lhd G$, N *is not* *k-nacci sequenceable*
G *is not k-nacci sequenceable*	$G = C_9 \times C_2$, $k = 2$ see [48]	$G = S_4$ $k = 2$
G *is k-nacci sequenceable*	$G = S_3$ $k = 3$	the subject of this section

Thus the notion of a k-nacci sequenceable group is quite specific to the group and is not necessarily inherited by any non-trivial (normal) subgroup. It must also be noted that a group G is k-nacci sequenceable if there exists at least one generating set that makes the k-nacci sequence contain every element of G. Thus to answer the question of Knox in the negative one must check the k-nacci condition over at most $\phi_k(N)$ generating sets, where $\phi_k(N)$ is the Eulerian function of N, $N \lhd G$, see [38].

To answer Knox's question several programs were written in the GAP computational algebra package [36] to calculate the k-nacci sequence of a seed set. In a systematic case by case study of groups of small order held in the library of the GAP system, proper normal subgroups were calculated. First it was checked if the group was k-nacci sequenceable for $3 \leq k \leq 7$ and, if it was, then the normal subgroups were then checked to see if any of them were k-nacci sequenceable.

The smallest example of a group that was k-nacci sequenceable, $3 \leq k \leq 7$, but whose proper normal subgroups were not k-nacci sequenceable was the non-

abelian group G of order 56 with $G/G' \cong C_7$ given as the following permutation group:

$$\begin{aligned} G = \langle & (1,31,7,49,25,54,44)(2,39,14,53,33,12,51)(3,42,17,50,36,37,23) \\ & (4,30,18,48,27,56,13)(5,32,9,40,16,47,24)(6,46,22,11,41,19,55) \\ & (8,38,26,52,35,20,21)(10,43,28,29,15,45,34), \\ & (1,38,23,28,53,41,16)(2,45,31,36,11,48,24)(3,39,44,18,52,32,6) \\ & (4,55,34,17,47,21,14)(5,29,22,8,56,42,25)(7,46,51,26,10,40,13) \\ & (9,37,30,15,20,49,33)(12,50,35,19,54,43,27)\rangle \end{aligned}$$

The unique proper normal subgroup N of G is isomorphic to C_2^3 and is given as the following permutation subgroup

$$\begin{aligned} N = \langle & (1,10)(2,17)(3,4)(5,20)(6,25)(7,8)(9,28)(11,12)(13,33)(14,15) \\ & (16,36)(18,19)(21,41)(22,23)(24,44)(26,27)(29,48)(30,31)(32,51) \\ & (34,35)(37,52)(38,39)(40,55)(42,43)(45,46)(47,56)(49,50)(53,54), \\ & (1,12)(2,19)(3,20)(4,5)(6,27)(7,28)(8,9)(10,11)(13,35)(14,36) \\ & (15,16)(17,18)(21,43)(22,44)(23,24)(25,26)(29,50)(30,51)(31,32) \\ & (33,34)(37,54)(38,55)(39,40)(41,42)(45,56)(46,47)(48,49)(52,53), \\ & (1,3)(2,7)(4,10)(5,11)(6,14)(8,17)(9,18)(12,20)(13,22)(15,25) \\ & (16,26)(19,28)(21,30)(23,33)(24,34)(27,36)(29,38)(31,41)(32,42) \\ & (35,44)(37,45)(39,48)(40,49)(43,51)(46,52)(47,53)(50,55)(54,56)\rangle \end{aligned}$$

We give the above generators for C_2^3 to reinforce the notion that $N \lhd G$.

Now G is 4-nacci sequenceable but no seed set of N, that generates N, makes N 4-nacci sequenceable. Thus we can answer the question posed in [48] in the negative.

Unfortunately the above method used to answer Knox's question does not shed any light on any deep reasons why this group failed to satisfy the conditions

of the question.

3 Practical computing considerations

3.1 Fibonacci length

In this section we will be concerned with designing practical procedures that will calculate the Fibonacci orbit or length of a given group.

We first examine if it is possible to design an algorithm that, given a finitely presented group, will output the Fibonacci length. To do this we first need some definitions:

Definition 3.1 A property $\mathcal{M}$ is called a *Markov property* if:

1. every group isomorphic to a group with property $\mathcal{M}$ also has property $\mathcal{M}$,
2. there exists a finitely presented group G with property $\mathcal{M}$,
3. there exists a finitely presented group G which cannot be embedded in a finitely presented group having property $\mathcal{M}$.

Famous examples of Markov properties are being trivial, free, nilpotent, having solvable word problem, etc. (See [58] for proofs and more examples.) It seems that many of the properties that one would like to know about a group defined by a finite presentation are Markov properties.

We now quote the following result.

Theorem 3.2 [Adian - Rabin, 1958] *If $\mathcal{M}$ is a Markov property, then there does not exist a decision process which will determine, for an arbitrary finite presentation, whether the group presented has property $\mathcal{M}$.*

Proof. See [58]. □

So we have:

Open question: Prove or disprove the following: There is no decision process to determine for an arbitrary finite presentation whether the group defined by the presentation has finite Fibonacci length.

Open question: If a group has solvable word problem, can one decide if it has finite Fibonacci length? Of course one could start a process going to test if the generators are equal to the successive elements of the Fibonacci orbit, but this is not guaranteed to take a finite length of time.

We know that a finite group has finite Fibonacci length.

To calculate the Fibonacci length of a given finitely presented group that is known to be finite we choose to use the following algorithm:

Algorithm 3.3 `Fibonacci length of a group presentation`
INPUT: a finitely presented group G defined by the presentation $\mathcal{P} = \langle X|R\rangle$.
OUTPUT: $LEN_X(G)$.

1: {We start by performing a Todd-Coxeter run over the trivial group}
2: $CosetTable(\mathcal{P}) \leftarrow$ `Todd − Coxeter`$(\mathcal{P},$ `TrivialGroup`$(\langle\mathcal{P}\rangle))$
3: **for all** $i \in \{1, 2, \ldots, |X|\}$ **do**
4: $\quad \sigma_i \leftarrow Column(CosetTable(\mathcal{P}))[i]$
5: **end for**
6: $G \leftarrow$ `Group`$(\sigma_{\mathtt{i}}|\mathtt{i} \in \{1, 2, \ldots, |\mathtt{X}|\})$
7: $List \leftarrow [\sigma_1, \sigma_2, \ldots, \sigma_{|X|}]$
8: $Stop \leftarrow$ `FALSE`
9: $LEN \leftarrow |X|$
10: **while** $Stop =$ `FALSE` **do**
11: $\quad x \leftarrow Product(List[1],\ List[2], \ldots, List[|X|])$

12: $LEN \leftarrow LEN + 1$

13: **for all** $i \in \{1, 2, \ldots, |X| - 1\}$ **do**

14: $List[i] \leftarrow List[i + 1]$

15: **end for**

16: $List[|X|] \leftarrow x$

17: **if** $List[1] = \sigma_1$ and $List[2] = \sigma_2$ and...and $List[|X|] = \sigma_{|X|}$ **then**

18: $Stop \leftarrow$ TRUE

19: **end if**

20: **end while**

21: **return** LEN

The above performs a Todd-Coxeter coset enumeration on $G = \langle\ X \mid R\ \rangle$ over the trivial subgroup and then uses the coset table to obtain permutation generators for a permutation group $PermG$ isomorphic to G. It is very easy and efficient to test equalities in $PermG$ e.g if $\sigma_1\sigma_2 = \sigma_3$, $\sigma_i \in S_n$, while it is computationally harder to test equalities in a presentation for G e.g. if $x_1x_2 = x_3$, $x_i \in X^*$.

The above algorithm has been implemented in GAP as the function **fpfl** and the code is presented in Appendix C.

Note if the above algorithm performs poorly for a given group then it may be expedient to run a program that uses the Knuth-Bendix procedure for testing equality of strings in algebraic objects; see [49] for a description of the process. Throughout the work carried out in this thesis we found it quicker to use the **fpfl** program than a program based on the Knuth-Bendix procedure. Of course, in general, there appears to be no gain in using Todd-Coxeter in preference to Knuth-Bendix, or vice versa.

3.2 Wall numbers

In contrast to the Fibonacci length of a group, calculating the Wall number of a given integer can be performed very quickly with the aid of a computer. In order to calculate the Wall number of a integer n we need the following results:

Definition 3.4 The *rank of apparition of* n, denoted by $ra(n)$, is the smallest positive integer $j > 0$ for which $f_j \equiv 0 \bmod n$. We now define $t(n)$ to be the rational satisfying $k(n) = ra(n)t(n)$.

We now give a result due to J. Vinson that lets us calculate the quantity $t(n)$:

Lemma 3.5 *Let p be an odd prime and let e be any positive integer. Then*

$$\begin{aligned} t(p^e) &= 4 \text{ if } 2 \nmid ra(p), \\ t(p^e) &= 1 \text{ if } 2 | ra(p) \text{ but } 4 \nmid ra(p), \\ t(p^e) &= 2 \text{ if } 4 | ra(p), \\ t(2^e) &= 2 \text{ for } e \geq 3 \text{ and } t(2) = t(2^2) = 1. \end{aligned}$$

Conversely, if q represents any prime, then $t(q^e) = 4$ implies $ra(q)$ is odd, $t(q^e) = 2$ implies $4 | ra(p)$ or $q = 2$ and $e \geq 3$, and $t(q^e) = 1$ implies $2 | ra(p)$ but $4 \nmid ra(p)$ or $q^e = 2$ or 4.

Proof. See [70] for the proof. □

So the problem of finding a formula to calculate $k(n)$ is reduced to finding a formula to calculate the rank of apparition of n.

In order to write a computer program to quickly calculate the Wall number of a given integer n we assume that $k(p^2) = pk(p)$ for all primes p. This has been checked for $p < 10^9$. This assumption together with the Lemma 3.5 lets us write two programs in GAP (**K** to calculate $k(p)$, for p a prime, and **Wall** to

calculate $k(m)$, for m composite). These programs together can calculate $k(n)$, where n runs from 3 to 1000, in 0.350 seconds of cpu time and it takes 0.340 seconds of cpu time to calculate $k(x)$ where $x = \prod_{i=1}^{168} p_i$, p_ℓ is the ℓth prime. The program **Wall** that calculates the Wall number of the given integer n has two time-consuming subprocesses, namely factorizing the number n and calculating the rank of apparition of the individual primes in the prime decomposition of n. If one wishes to calculate the Wall number of $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}$ with p_i being the *ith* prime, $10^9 < p_l$ for $l \leq t$, $\alpha_l \neq 0$ and $\alpha_i \in \mathbb{N} \cup \{0\}$ then one uses the **K** program that only uses Lemma 3.5.

Chapter 3

The Fibonacci length of metacyclic groups

1 Introduction

As mentioned earlier, the Fibonacci length of a general cyclic group G was calculated in 1960 by D. D. Wall [71]. A natural generalization of this problem, calculating the Fibonacci length of a general abelian group, was studied in 1985 by H. J. Wilcox [74]. Since this date the study of the Fibonacci lengths of finite groups has moved on in several different directions to include certain nilpotent groups (Aydin and Dikici [3]), p-groups (Aydin and Smith [4]) and simple groups (C. M. Campbell, H. Doostie and E. F. Robertson [19]). Most of the above analysis is carried out on two-generated finite groups. In this chapter we intend to widen the class of groups studied to include two infinite families of finite metacyclic groups. The results of this chapter indicate a possible connection between the Fibonacci length of cyclic groups and certain metacyclic groups since the lengths of the metacyclic groups considered turn out to be Wall numbers.

Some of the results in this section will appear in a paper entitled "Fibonacci

length for certain metacyclic groups" by C. M. Campbell, P. P. Campbell, H. Doostie and E. F. Robertson, see [16].

2 Preliminaries

We first start by defining metacyclic groups and giving some well known results concerning them.

Definition 2.1 A group G is called *metacyclic* if it has a cyclic normal subgroup N such that G/N is also cyclic.

So a metacyclic group G is an extension of a cyclic group N, $N \cong N_1$, by a cyclic group Q, $Q \cong G/N_1$.

It is well known that the group $G_{m,n,r,s}$ defined by the presentation

$$\mathcal{P}_{m,n,r,s} = \langle\, a, b \mid a^m = 1, b^{-1}ab = a^r, b^n = a^s \,\rangle,$$

is a metacyclic groups of order mn where $m, n, r, s \in \mathbb{N}$ and $r^n \equiv 1 \pmod{m}$, $rs \equiv s \pmod{m}$. Moreover every metacyclic group has a presentation of this form; see [45]. If $s = m/(m, r-1)$ then $G_{m,n,r,s}$ has a presentation

$$\mathcal{Q}_{m,n,r,s} = \langle\, a, b \mid [b^{-1}, a^{-t}] = a^{(m,r-1)}, a^s b^n = 1 \,\rangle.$$

where, if $(m, r-1) = u(r-1) + vm$ and w is the largest factor of m coprime to u, then $t = u + ws$; see [12] and [13] for details.

It is known that the Schur multiplier of the group $G_{m,n,r,s}$ is the cyclic group C_k of order k, where $k = s(m, r-1)/m$. These results together give us the following:

Theorem 2.2 *Finite metacyclic groups are efficient groups with efficient pre-*

sentations

$$\begin{aligned} &\mathcal{P}_{m,n,r,s} && \text{if } s \neq m/(m, r-1) \\ &\mathcal{Q}_{m,n,r,s} && \text{if } s = m/(m, r-1). \end{aligned}$$

Presentations of metacyclic groups are still being investigated. In fact in recent work, see for example [5], it is shown that:

Theorem 2.3 *Finite metacyclic groups are efficient as semigroups, with efficient semigroup presentations:*

$$\begin{aligned} &\langle\, a, b \mid a^{m+1} = a, a^{m-r}ba = b, a^{m-s} = b^n \,\rangle && \text{if } s \neq m/(m, r-1) \\ &\langle\, a, b \mid a^{(m,r-1)+t}b^{(m,r-1)n+1}a^{m-t} = b, a^s b^n a = a \,\rangle && \text{if } s = m/(m, r-1). \end{aligned}$$

3 A family of presentations due to R. H. Fox

In 1956 while working on a problem in topology R. H. Fox had reason to investigate the group defined by the presentation

$$\langle\, a, b \mid ab^2 = b^3a, ba^2 = a^3b \,\rangle.$$

Later work was carried out by Benson and Mendelson [11] on a generalization of this presentation, namely

$$\langle\, a, b \mid ab^n = b^{n+1}a, ba^n = a^{n+1}b \,\rangle.$$

In 1976 C. M. Campbell and E. F. Robertson, see [21], carried out investigations into the presentation

$$\langle\, a, b \mid ab^n = b^\ell a, ba^n = a^\ell b \,\rangle,$$

which include the class of presentations investigated by Benson and Mendelson, and thus the Fox presentation. In their paper Campbell and Robertson showed that:

Theorem 3.1 *Let $G_{n,\ell}$ be the group defined by the presentation*

$$\langle\, a, b \mid ab^n = b^\ell a, ba^n = a^\ell b \,\rangle.$$

Then if

(1) $(n, \ell) \neq 1, G_{n,\ell}$ *is infinite,*

(2) $(n, \ell) = 1, G_{n,\ell}$ *is finite of order* $|\ell - n|^3$.

They also calculated properties of the generators.

Theorem 3.2 *If $G_{n,\ell}$ is defined by the presentation*

$$\langle\, a, b \mid ab^n = b^\ell a, ba^n = a^\ell b \,\rangle.$$

Then

(1) *if* $(\ell, n) = 1, |a| = |b| = (\ell - n)^2$,

(2) *if* $(\ell, n) = 1, a^{\ell-n} = b^{n-\ell}$.

To find the Fibonacci length of $G_{n,\ell}$ we will first partition the family $\{G_{n,\ell} : n, \ell\}$ into isomorphism classes and then find a standard form for the Fibonacci orbit of a general entry in each isomorphism class. Using this standard form we can construct a normal form for the elements of $G_{n,l}$. Finally we shall use number theory to find the minimal period of the Fibonacci orbit.

We start by proving that certain $G_{n,\ell}$ are in fact isomorphic:

Lemma 3.3 *Let $G_{n,\ell}$ be the group defined by the presentation*

$$\langle\, a, b \mid ab^n = b^\ell a, ba^n = a^\ell b \,\rangle,$$

then:

(1) *for every* $\ell \geq 3, G_{1,\ell} \cong G_{1,2-\ell}$;

(2) *for* $i \geq 2$ *and* $(n, i) = 1, G_{n,n+i} \cong G_{1,1+i}$.

Proof. We first show that $G_{1,\ell} \cong G_{1,2-\ell}$, for $\ell \geq 3$.

Now $G_{1,\ell}$ is defined by the presentation $\langle\, a, b \mid ab = b^\ell a, ba = a^\ell b \,\rangle$. First examine the relation

$$b = a^{-1} b^\ell a.$$

Raise this to the power $2 - \ell$ to get

$$b^{2-\ell} = a^{-1} b^{\ell(2-\ell)} a.$$

In $G_{1,\ell}$ the order of the generators is $(\ell - 1)^2$ so

$$b^{2-\ell} = a^{-1} \underline{b^{2\ell-\ell^2}} a = a^{-1} b a.$$

Likewise if we look at the other relator we have

$$a = b^{-1} a^\ell b$$

so

$$a^{2-\ell} = b^{-1} a^{\ell(2-\ell)} b = b^{-1} \underline{a^{2\ell-\ell^2}} b = b^{-1} a b.$$

Thus we have

$$G_{1,\ell} = \langle\, a, b \mid ab = b^\ell a, ba = a^\ell b, ab^{2-\ell} = ba, ba^{2-\ell} = ab \,\rangle.$$

Now we show that the last two relations imply the first two relations. Let $\mathcal{H}_\ell$ be the presentation

$$\langle\, a, b \mid ab^{2-\ell} = ba, ba^{2-\ell} = ab \,\rangle.$$

Now the generators of $\mathcal{H}_\ell$ have order $(1 - l)^2$. We now, in essence, 'reverse' the previous argument. Examining the relation

$$b^{2-\ell} = a^{-1} b a$$

we raise it to the power ℓ to give

$$b^{2\ell-\ell^2} = a^{-1}b^{\ell}a.$$

So

$$b = a^{-1}b^{\ell}a$$

and we have shown that in $\mathcal{H}_\ell$ the relations $ab = b^{\ell}a$ and $ba = a^{\ell}b$ hold.

We use Tietze transformations to introduce a new set of generators

$$\begin{aligned} G_{1,\ell} &\cong \langle\, a, b, x, y \mid ab^{2-\ell} = ba, ba^{2-\ell} = ab, x = b^{-1}, y = a^{-1} \,\rangle \\ &\cong \langle\, x, y \mid y^{-1}x^{\ell-2} = x^{-1}y^{-1}, x^{-1}y^{\ell-2} = y^{-1}x^{-1} \,\rangle \\ &\cong \langle\, x, y \mid yx = x^{2-\ell}y, xy = y^{2-\ell}x \,\rangle \\ &\cong G_{1,2-\ell}. \end{aligned}$$

The above transformations are all reversible and so the first statement of the proof is complete.

We now show that $G_{n,n+i} \cong G_{1,1+i}$.

Let $G_{n,n+i}$ be the group defined by the presentation

$$\langle\, a, b \mid ab^n = b^{n+i}a, ba^n = a^{n+i}b \,\rangle.$$

Suppose $(n, i) = 1$ so $\alpha n + \beta i = 1$ for some $\alpha, \beta \in \mathbb{Z}$.

First we show that $aba^{-1} = b^{1+\alpha i}$ holds in $G_{n,n+i}$. From $ab^n a^{-1} = b^{n+i}$ we have

$$ab^{\alpha n}a^{-1} = b^{\alpha n+\alpha i}$$

so $ab^{1-\beta i}a^{-1} = b^{1-\beta i+\alpha i}$. But b^i is central in $G_{n,n+i}$, by Theorem 3.2 (2), so

$$aba^{-1} = b^{1+\alpha i}.$$

Now, by Theorem 3.2 (1), a and b have order i^2 so $G_{n,n+i} = \langle\, a^n, b^n \,\rangle$ since $(n,i) = 1$. Put $A = a^n, B = b^n$. Then $ABA^{-1} = a^n b^n a^{-n} = b^{n(1+\alpha i)^n} = B^{(1+\alpha i)^n}$. But $B^{i^2} = 1$ we have $B^{(1+\alpha i)^n} = B^{1+n\alpha i} = B^{1+(1-\beta i)i} = B^{1+i}$. Hence $ABA^{-1} = B^{1+i}$ and similarly $BAB^{-1} = A^{1+i}$. Since $G_{n,n+i} = \langle\, A, B \,\rangle$ and the group with presentation $\langle A, B | ABA^{-1} = B^{1+i}, BAB^{-1} = A^{1+i} \,\rangle$ has order $i^3 = |G_{n,n+i}|$ the result follows. □

The following result is easy to see but we include the proof for completeness.

Theorem 3.4 *For integers n and ℓ, $G_{n,\ell} \cong G_{\ell,n}$.*

Proof. Let n and ℓ be given integers and let

$$\begin{aligned} \mathcal{P}_1 &= \langle\, a, b \mid ab^n = b^\ell a, ba^n = a^\ell b \,\rangle \\ \mathcal{P}_2 &= \langle\, x, y \mid xy^\ell = y^n x, yx^\ell = x^n y \,\rangle. \end{aligned}$$

We wish to use Tietze transformations to obtain $\mathcal{P}_2$ from $\mathcal{P}_1$, and vice-versa. So we have

$$\begin{aligned} \mathcal{P}_1 &= \langle\, a, b, u, v \mid ab^n = b^\ell a, ba^n = a^\ell b, u = a^{-1}, v = y^{-1} \,\rangle \\ &= \langle\, a, b, u, v \mid ab^n = b^\ell a, ba^n = a^\ell b, u = a^{-1}, v = b^{-1}, u^{-1}v^{-n} = v^{-\ell}u^{-1}, v^{-1}u^{-n} = u^\ell v^{-1} \,\rangle \\ &= \langle\, a, b, u, v \mid ab^n = b^\ell a, ba^n = a^\ell b, u = a^{-1}, v = b^{-1}, uv^\ell = v^n u, vu^\ell = u^n v \,\rangle \\ &= \langle\, u, v \mid uv^\ell = v^n u, vu^\ell = u^n v \,\rangle \\ &= \mathcal{P}_2. \end{aligned}$$

The reverse of the transformations also hold so we have shown that $G_{n,\ell} \cong G_{\ell,n}$. □

Remark 3.5 If $(\ell, n) = 1$ by the previous lemmas we may assume without loss of generality that $n < \ell$. Then we have shown that $G_{n,\ell} = G_{n,n+i} \cong G_{1,1+i}$ for

some positive integer i, $i \geq 2$. We note here that the group $G_{1,2}$ is isomorphic to the trivial group and we don't consider it here. So from this point on every time we mention G_j in this section we will assume that $j \geq 3$. In fact from this point on we will only be interested in calculating $LEN_{\{a,b\}}(G_{1,j})$ for all possible j's, $j \geq 3$.

As a consequence of the previous remark we shall write G_j to denote the group $G_{1,j}$.

Remark 3.6 We now use the above results to create a table illustrating the 'behaviour' of a small selection of groups. We calculate the results for all groups $G_{n,\ell}$, where $1 \leq n \leq 10$ and $3 \leq \ell \leq 10$. The symbol ∞ is used to mean a group of infinite order and $\{ \text{ id } \}$ to mean the trivial group.

$n \setminus \ell$	3	4	5	6	7	8	9	10
1	$G_{1,3}$	$G_{1,4}$	$G_{1,5}$	$G_{1,6}$	$G_{1,7}$	$G_{1,8}$	$G_{1,9}$	$G_{1,10}$
2	$\{ \text{ id } \}$	∞	$G_{1,4}$	∞	$G_{1,6}$	∞	$G_{1,8}$	∞
3	∞	$\{ \text{ id } \}$	$G_{1,3}$	∞	$G_{1,5}$	$G_{1,6}$	∞	$G_{1,8}$
4	$\{ \text{ id } \}$	∞	$\{ \text{ id } \}$	∞	$G_{1,4}$	∞	$G_{1,6}$	∞
5	$G_{1,3}$	$\{ \text{ id } \}$	∞	$\{ \text{ id } \}$	$G_{1,3}$	$G_{1,4}$	$G_{1,5}$	∞
6	∞	∞	$\{ \text{ id } \}$	∞	$\{ \text{ id } \}$	∞	∞	∞
7	$G_{1,5}$	$G_{1,4}$	$G_{1,3}$	$\{ \text{ id } \}$	∞	$\{ \text{ id } \}$	$G_{1,3}$	$G_{1,4}$
8	$G_{1,6}$	∞	$G_{1,4}$	∞	$\{ \text{ id } \}$	∞	$\{ \text{ id } \}$	∞
9	∞	$G_{1,6}$	$G_{1,5}$	∞	$G_{1,3}$	$\{ \text{ id } \}$	∞	$\{ \text{ id } \}$
10	$G_{1,8}$	∞	∞	∞	$G_{1,4}$	∞	$\{ \text{ id } \}$	∞

We now show that every element in the Fibonacci orbit of G_ℓ, where $\ell \in \mathbb{N}$, has a standard form.

Lemma 3.7 *In G_ℓ every element in the Fibonacci orbit, $(x_n)_{n=0}^{\infty}$, can be written in the form $x_n = a^{\alpha_n} b^{f_n}$ where $\alpha_n = \alpha_{n-2} + \alpha_{n-1}\ell^{f_{n-2}}$ for $n \geq 2$, with $\alpha_0 = 1$ and $\alpha_1 = 0$.*

Proof. We use induction on n. Clearly when $n = 0$ and $n = 1$ the elements x_0 and x_1 of the Fibonacci orbit are of the form $x_0 = a^{\alpha_0} b^{f_0} = a$ and $x_1 = a^{\alpha_1} b^{f_1} = b$.

Now assume that the result hold for all elements in the Fibonacci orbit less than x_n. So by definition we have

$$\begin{aligned} x_n &= x_{n-2}x_{n-1}, \\ &= a^{\alpha_{n-2}} b^{f_{n-2}} a^{\alpha_{n-1}} b^{f_{n-1}}. \end{aligned}$$

We now rewrite this last term using the relation $ba = a^\ell b$. Using this relation we have, for general integers i and j:

$$b^i a^j = b^{i-1}\underline{ba}a^{j-1} = b^{i-1}a^\ell \underline{ba}a^{j-2} = b^{i-1}a^{2\ell}\underline{ba}a^{j-3} = \ldots$$
$$\ldots = b^{i-1}a^{j\ell}b = b^{i-2}\underline{ba}a^{j\ell-1}b = \ldots = b^{i-2}a^{j\ell^2}b^2 = \ldots = a^{j\ell^i}b^i.$$

So using this we have

$$\begin{aligned} x_n &= a^{\alpha_{n-2}}\underline{b^{f_{n-2}}a^{\alpha_{n-1}}}b^{f_{n-1}}, \\ &= a^{\alpha_{n-2}+\alpha_{n-1}\ell^{f_{n-2}}} b^{f_{n-2}} b^{f_{n-1}}, \\ &= a^{\alpha_n} b^{f_n}. \end{aligned}$$

So the result holds. □

We now go about solving the recurrence relation for α_n modulo $(\ell-1)^2$, where $(\alpha_n)_{n=0}^{\infty}$ is the sequence from Lemma 3.7. We first need the following elementary result

Lemma 3.8 *For integers ℓ and m, $\ell^m \equiv 1 + m(\ell-1) \bmod (\ell-1)^2$.*

Proof. Write $\ell^m = (1 + (\ell - 1))^m$ then, using the binomial theorem, we have $(1 + (\ell - 1))^m = \sum_{j=0}^{m} \binom{m}{j} (\ell - 1)^j$ and reducing this sum modulo $(\ell - 1)^2$ gives $(1 + (\ell - 1))^m \equiv 1 + m(\ell - 1) \bmod (\ell - 1)^2$. □

Lemma 3.9 *Let the sequence* $(\alpha_n)_{n=0}^{\infty}$ *be as defined in* Lemma 3.7. *Let* $\alpha_m \in (\alpha_n)_{n=0}^{\infty}$ *be an arbitrary element from the sequence. Then*

$$\alpha_m \equiv \left(f_{m-1} + (\ell - 1) \sum_{i=1}^{m-2} f_{m-1-i} f_i^2 \right) \bmod (\ell - 1)^2$$

where f_m *is the* m*th Fibonacci number.*

Proof. Using Lemmas 3.7 and 3.8 we have,

$$\alpha_m = \alpha_{m-2} + \alpha_{m-1} \ell^{f_{m-2}} \equiv (\alpha_{m-2} + \alpha_{m-1} + (\ell - 1) f_{m-2} \alpha_{m-1}) \bmod (\ell - 1)^2.$$

We use induction on m. The result clearly holds for $m = 0$ and $m = 1$. Now assume it holds for $m - 1$ and $m - 2$. We have, working mod $(\ell - 1)^2$,

$$\begin{aligned}
\alpha_m &\equiv \alpha_{m-1} + \alpha_{m-2} + (\ell - 1) f_{m-2} \alpha_{m-1} \\
&\equiv f_{m-2} + (\ell - 1) \sum_{i=1}^{m-3} f_{m-2-i} f_i^2 + f_{m-3} + (\ell - 1) \sum_{i=1}^{m-4} f_{m-3-i} f_i^2 + (\ell - 1) f_{m-2}^2 \\
&\equiv f_{m-2} + (\ell - 1) \sum_{i=1}^{m-3} f_{m-2-i} f_i^2 + f_{m-3} + (\ell - 1) \sum_{i=1}^{m-3} f_{m-3-i} f_i^2 + (\ell - 1) f_{m-2}^2 \\
&\equiv f_{m-1} + (\ell - 1) \sum_{i=1}^{m-3} f_{m-1-i} f_i^2 + (\ell - 1) f_{m-2}^2 \\
&\equiv f_{m-1} + (\ell - 1) \sum_{i=1}^{m-2} f_{m-1-i} f_i^2
\end{aligned}$$

and thus the result holds. □

Before we present the main results of this section we need to develop some results concerning Fibonacci numbers and sums of Fibonacci numbers where the indices run over Wall numbers.

Lemma 3.10 *For any positive integers n and $t \geq 2$ we have*

$$f_{k(t)+n} \equiv f_n \bmod t.$$

Proof. This follows directly from the definition of the Wall number. □

This leads us to

Corollary 3.11 *For positive integers n, m and t, $m \geq 1, t \geq 2$, we have:*

$$f_{mk(t)+n} \equiv f_n \bmod t.$$

Proof. Let n, m, t be positive integers with $m \geq 1, t \geq 2$ then:

$$\begin{aligned} f_{mk(t)+n} &= f_{k(t)+((m-1)k(t)+n)} \\ &\equiv f_{(m-1)k(t)+n} \bmod t \\ &\cdots \\ &\equiv f_n \bmod t. \end{aligned}$$

□

Lemma 3.12 *For any integer $t \geq 2$ we have*

$$\sum_{i=1}^{k(t)} f_{k(t)-i-1} f_i^2 \equiv 0 \bmod t.$$

Proof. This can be seen to hold from the results of [4]. □

Now we give the following results

Corollary 3.13 *The following are divisible by the positive integer t*

(i) $$\sum_{i=1}^{k(t)-1} f_{k(t)-i-1} f_i^2$$

(ii) $$\sum_{i=1}^{k(t)-2} f_{k(t)-i-1} f_i^2.$$

Proof. The first result can be seen to hold by noting that when $i = k(t)$,

$$f_{k(t)-i-1}f_i^2 = f_{k(t)-k(t)-1}f_{k(t)}^2 \equiv f_{-1}f_0^2 \equiv 0 \bmod t$$

by Lemma 3.10. The result now follows from Lemma 3.12.

Likewise (ii) holds since when $i = k(t) - 1$, we have

$$f_{k(t)-i-1}f_i^2 = f_{k(t)-(k(t)-1)-1}f_{k(t)-1}^2 \equiv f_0 f_{-1}^2 \equiv 0 \bmod t.$$

Now use (i) and Lemma 3.12 to deduce (ii). □

Having a standard form for the entries in the Fibonacci orbit we now produce a normal form for the elements of the group.

Lemma 3.14 *Every element in the group G_ℓ can be written uniquely in the form*

$$a^\beta b^\gamma z^\delta,$$

where $0 \leq \beta, \gamma, \delta < (\ell - 1)$ and $z = a^{\ell-1}$.

Proof. That every element in G_ℓ can be written in this form follows from Theorem 3.2 (1) and (2). That this expression is unique follows since there are $(\ell - 1)^3$ elements of this form and G_ℓ has order $(\ell - 1)^3$. □

So now we can put the entries in the Fibonacci orbit into this form as follows.

Lemma 3.15 *The term x_n in the Fibonacci orbit of G_ℓ can be written in the form $a^\beta b^\gamma z^\delta$ where $z = a^{\ell-1}$ and*

$$\begin{aligned}
\beta &= f_{n-1} \bmod (\ell - 1), \\
\gamma &= f_n \bmod (\ell - 1), \\
\delta &= \Big(\sum_{i=1}^{n-2} f_{n-1-i}f_i^2 + \\
&\quad [f_{n-1} - (f_{n-1} \bmod (\ell - 1)) - f_n + (f_n \bmod (\ell - 1))]/(\ell - 1)\Big) \bmod (\ell - 1).
\end{aligned}$$

Proof. To see this we first write a member of the Fibonacci orbit x_n in a standard form using Lemmas 3.7 and 3.9, then we use the fact that $a^{\ell-1} = b^{1-\ell}$ so

$$\begin{aligned} x_n &= a^{f_{n-1}+(\ell-1)\sum_{i=1}^{n-2} f_{n-1-i}f_i^2} b^{f_n}, \\ &= a^{f_{n-1} \bmod (\ell-1)} b^{f_n \bmod (\ell-1)} a^{f_{n-1}-f_{n-1} \bmod (\ell-1)} a^{(\ell-1)\sum_{i=1}^{n-2} f_{n-1-i}f_i^2} a^{-(f_n - f_n \bmod (\ell-1))}, \\ &= a^{f_{n-1} \bmod (\ell-1)} b^{f_n \bmod (\ell-1)} a^{f_{n-1}-f_{n-1} \bmod (\ell-1)-f_n+f_n \bmod (\ell-1)+(\ell-1)\sum_{i=1}^{n-2} f_{n-1-i}f_i^2}. \end{aligned}$$

The result now follows by taking out a common factor of $(\ell - 1)$ from the last power of a and then reducing it modulo $(\ell - 1)$. □

Now $LEN(G_\ell)$ is obviously a multiple of $k(\ell - 1)$ (the power of b in the orbit is a Fibonacci number). We complete this section by showing that $LEN(G_\ell) = k((\ell - 1)^2)$.

Theorem 3.16 *For every integer $\ell \geq 2$, $LEN(G_\ell) = k((\ell - 1)^2)$.*

Proof. Let $n = LEN(G_\ell) = mk(\ell - 1)$ for some natural number m. We start with some observations:

$$\begin{aligned} f_{n-1} &\equiv 1 \bmod (\ell - 1) \text{ by Corollary 3.11,} \\ f_n &\equiv 0 \bmod (\ell - 1) \text{ by Corollary 3.11,} \\ f_{n+1} &\equiv 1 \bmod (\ell - 1) \text{ by Corollary 3.11,} \\ \sum_{i=1}^{n-2} f_{n-1-i}f_i^2 &\equiv 0 \bmod (\ell - 1) \text{ by Corollaries 3.11, 3.13 and repeated use of Lemma 3.12,} \\ \sum_{i=1}^{n-1} f_{n-1-i}f_i^2 &\equiv 0 \bmod (\ell - 1) \text{ by Corollaries 3.11, 3.13 and repeated use of Lemma 3.12.} \end{aligned}$$

So it suffices to show that both

$$[f_{n-1} - (f_{n-1} \bmod (\ell - 1))]/(\ell - 1) - [f_n - (f_n \bmod (\ell - 1))]/(\ell - 1),$$

and

$$[f_n - (f_n \bmod (\ell-1))]/(\ell-1) - [f_{n+1} - (f_{n+1} \bmod (\ell-1))]/(\ell-1),$$

are multiples of $\ell - 1$. To do this we show that

$$(f_{n-1} - 1 - f_n)/(\ell-1)^2$$

and

$$(f_n - f_{n+1} + 1)/(\ell-1)^2$$

are integers. But

$$(f_{n-1} - 1 - f_n)/(\ell-1)^2 \;=\; (-f_{n-2} - 1)/(\ell-1)^2,$$

which is an integer since

$$f_{n-2} \;\equiv\; -1 \bmod (\ell-1)^2.$$

Likewise

$$(f_n - f_{n+1} + 1)/(\ell-1)^2 \;=\; (-f_{n-1} + 1)/(\ell-1)^2,$$

which is an integer since

$$f_{n-1} \;\equiv\; 1 \bmod (\ell-1)^2.$$

The smallest n, $n \geq 0$, satisfying these equations and having $k(\ell-1)$ as a factor is $k((\ell-1)^2)$. So we have $LEN(G_\ell) = k((\ell-1)^2)$. □

We now give examples of calculating the Fibonacci length of G_ℓ via the **fpfl** GAP program and a program specifically designed to calculate a Wall number (It uses Vinson's rank of apparition method and assumes that $k(p^2) = pk(p)$. This has been checked for all primes p, $p \leq 10^9$).

ℓ	$\mathbf{fpfl}(G_\ell)$	time*	$k((\ell-1)^2)$	time*
4	24	110	24	0
5	24	120	24	0
6	100	120	100	0
7	24	130	24	0
8	112	110	112	0
9	96	130	96	0
10	216	150	216	0
51	7500	126610	7500	0
71	8400	294190	8400	0
99	16464	1118100	16464	0

$*$ Time is in milliseconds of cpu time.

4 The Fibonacci groups $F(r,2)$, r odd

Here we investigate the Fibonacci length of the Fibonacci groups $F(r,2)$, r odd, defined by the presentation

$$\langle\, a_1, a_2 \mid (a_1a_2)^{(r-1)/2} = a_2a_1^{-1}, (a_2a_1)^{(r-1)/2} = a_1a_2^{-1} \,\rangle.$$

The Fibonacci groups $F(r,2)$, where $r \in \mathbb{N}$, were amongst the first family of Fibonacci groups to be studied. Some elementary results concerning the groups $F(r,2)$, $r \in \mathbb{N}$, are listed below:

Theorem 4.1 *Let $F(r,n)$ be the Fibonacci group defined by the presentation*

$$\langle\, a_1, a_2, \ldots, a_n \quad \mid \quad a_1a_2a_3\ldots a_r = a_{r+1},\ a_2a_3a_4\ldots a_{r+1} = a_{r+2}, \ldots,$$
$$a_{n-1}a_na_1\ldots a_{r-2} = a_{r-1},\ a_na_1a_2\ldots a_{r-1} = a_r \,\rangle.$$

Then

(i) $F(r,n)$ *is metacyclic of order* $r^n - 1$ *if* $r \equiv 1 \bmod n$,

(ii) *if* $r > 1$ *and* n *is a divisor of* r, *then* $F(r,n) \cong C_{r-1}$,

(iii) *for all* $m \geq 1$, $F(2m+1,2)$ *is isomorphic to the metacyclic group defined by the presentation*

$$\langle a, b \mid a^2 = b^{m+1}, a^{-1}ba = b^{2m+1}, b^{2m^2+2m} = 1 \rangle$$

(iv) *the generators of the Fibonacci group* $F(r,2)$, *where* r *is odd, have order* $2(r-1)$.

Proof. For proofs see [46] and [64]. □

In the light of the above theorem, parts (i) and (ii), we will restrict ourselves to considering $F(r,2)$ where r is an odd number.

We will proceed as before by finding a form for the Fibonacci orbit and then use properties of this form to find the Fibonacci length of the groups defined by the above presentations. Again we find that the Fibonacci length is linked to certain Wall numbers.

It is easy to see that $F(3,2) \cong Q_8$, the quaternion group of order eight. In [19] it is proved that $LEN(Q_8)_{\{a,b\}} = 3$ for any generating pair $\{a,b\}$.

We will first need the following relation that follows from the presentation for $F(r,2)$.

Lemma 4.2 *The relations of* $F(r,2)$ *imply the relation*

$$a_1^2 = a_2^2.$$

Proof. From $(a_1a_2)^{(r-1)/2} = a_2a_1^{-1}$ we get $(a_1a_2)^{(r-1)/2}a_1 = a_2$ so

$$\begin{aligned} a_2 &= (a_1a_2)^{(r-1)/2}a_1 \\ &= a_1(a_2a_1)^{(r-1)/2}. \end{aligned}$$

But the second relation, namely $(a_2a_1)^{(r-1)/2} = a_1a_2^{-1}$, gives

$$a_2 = a_1a_1a_2^{-1}$$

or

$$a_1^2 = a_2^2$$

and thus the result holds. □

Now we find a standard form for the Fibonacci orbit $x_0, x_1, \ldots$ of $F(r,2)$, $r \geq 5$.

Lemma 4.3 *Let $x_0, x_1, \ldots$ be the Fibonacci orbit of $F(r,2)$ with $x_0 = a_1, x_1 = a_2$. Then*

$$x_w = \begin{cases} a_1^{f_{w+1}}, & w \equiv 0 \bmod 6, \\ a_1^{-1+f_{w+1}}a_2, & w \equiv 1 \bmod 6, \\ a_1^{-1+f_{w+1}}a_2, & w \equiv 2 \bmod 6, \\ a_1^{-3+f_{w+1}}a_2a_1a_2, & w \equiv 3 \bmod 6, \\ a_1^{-1+f_{w+1}}a_2, & w \equiv 4 \bmod 6, \\ a_1^{-2+f_{w+1}}a_2a_1, & w \equiv 5 \bmod 6, \end{cases}$$

for every $w \geq 0$.

Proof. We use induction on w.

We begin with the anchor case

$$\begin{aligned}
x_0 &= a_1 = a_1^{f_1}, \\
x_1 &= a_2 = a_1^{f_2-1}a_2, \\
x_2 &= a_1a_2 = a_1^{f_3-1}a_2, \\
x_3 &= a_2a_1a_2 = a_1^{f_4-3}a_2a_1a_2, \\
x_4 &= a_1\underline{a_2a_2}a_1a_2 = a_1^4a_2 = a_1^{f_5-1}a_2, \\
x_5 &= a_2a_1a_2\underline{a_1^4}a_2 = a_1^4a_2a_1\underline{a_2^2} = a_1^4a_2a_1\underline{a_1^2} = a_1^6a_2a_1.
\end{aligned}$$

Now assume that the result holds for all integers less than or equal to w, where $w \equiv 5 \bmod 6$. Then we have

$$\begin{aligned}
x_{w-1} &= a_1^{f_{w-1}}a_2 \\
x_w &= a_1^{f_{w+1}-2}a_2a_1.
\end{aligned}$$

Using the facts that the equation $a_1^2 = a_2^2$ holds in $F(r,2)$ and when $i \equiv 0 \bmod 3$ f_i is an even integer we may continue the induction:

$$\begin{aligned}
x_{w+1} &= a_1^{f_w-1}a_2\underline{a_1^{f_{w+1}-2}}a_2a_1 = a_1^{f_w-1+f_{w+1}-2}\underline{a_2^2}a_1 = a_1^{f_{w+2}-3}a_1^3 = a_1^{f_{w+2}} \\
x_{w+2} &= a_1^{f_{w+1}-2}a_2a_1a_1^{f_{w+2}} = a_1^{f_{w+1}-2}a_2\underline{a_1^{f_{w+2}+1}} = a_1^{f_{w+1}-2+f_{w+2}+1}a_2 = a_1^{f_{w+3}-1}a_2 \\
x_{w+3} &= a_1^{f_{w+2}}a_1^{f_{w+3}-1}a_2 = a_1^{f_{w+2}+f_{w+3}-1}a_2 = a_1^{f_{w+4}-1}a_2 \\
x_{w+4} &= a_1^{f_{w+3}-1}a_2\underline{a_1^{f_{w+4}-1}}a_2 = a_1^{f_{w+3}-1+f_{w+4}-2}a_2a_1a_2 = a_1^{f_{w+5}-3}a_2a_1a_2 \\
x_{w+5} &= a_1^{f_{w+4}-1}a_2\underline{a_1^{f_{w+5}-3}}a_2a_1a_2 = \underline{a_1^{f_{w+4}-1+f_{w+5}-3}a_2^2}a_1a_2 = \underline{a_1^{f_{w+6}-4}a_1^2a_1}a_2 = a_1^{f_{w+6}-1}a_2 \\
x_{w+6} &= a_1^{f_{w+5}-3}a_2a_1a_2\underline{a_1^{f_{w+6}-1}}a_2 = \underline{a_1^{f_{w+5}-3+f_{w+6}-1}}a_2a_1\underline{a_2a_2} = a_1^{f_{w+7}-4}a_2a_1\underline{a_1^2} = a_1^{f_{w+7}-2}a_2a_1
\end{aligned}$$

Thus the induction holds and the elements of the Fibonacci orbit have the required form. □

Now we know the Fibonacci orbit and the orders of the elements. We now turn our attention to finding some properties of the Fibonacci length.

Lemma 4.4 *For odd r, $r \geq 5$, the Fibonacci length of $F(r,2)$ is the least integer m such that $m \equiv 0 \bmod 6$, $f_{m+1} \equiv 1 \mod 2(r-1)$ and $f_{m+2} \equiv 1 \mod 2(r-1)$.*

Proof. We know from the definition that $m = LEN(F(r,2))$ if and only if m is the least integer such that $x_m = x_0 = a_1$ and $x_{m+1} = x_1 = a_2$. In the orbit we see that for $x_m = a_1$ we need $LEN(F(r,2))$ to be a multiple of 6 and this will also require $f_{m+1} \equiv 1 \bmod |a_1| = 2(r-1)$, i.e $m = k(2(r-1))$, and $x_{m+1} = x_1 = a_2$ means that $f_{m+2} \equiv 1 \bmod 2(r-1)$ must hold. □

Now we know enough properties of the Fibonacci length to calculate it.

Theorem 4.5 *For odd $r \geq 5$ we have*

$$LEN(F(r,2)) = k(2(r-1)).$$

Proof. By Lemma 4.4 the Fibonacci length, m say, of $F(r,2)$ must satisfy $f_{m+1} \equiv 1 \bmod (2(r-1))$, $f_{m+2} \equiv 1 \bmod (2(r-1))$ and $m \equiv 0 \bmod 6$. By the definition of $k(n)$ the first time that $f_{m+1} \equiv 1 \bmod (2(r-1))$ and $f_{m+2} \equiv 1 \bmod (2(r-1))$ is when $m = k(2(r-1))$.

Now, by Lemma 4.4, to complete the proof we need to show that 6 divides $k(2(r-1))$ for all odd $r \geq 5$. Since $k(2) = 3 \neq 6 = k(4)$, we may deduce

$$k(2^t) = 2^{t-1}.k(2) = 2^{t-1}.3 = 6.2^{t-2}.$$

Finally from the prime factorization $2(r-1) = 2^t \prod p_i^{e_i}$, where $t \geq 2$ and $p_i \neq 2$, we obtain $k(2(r-1)) = \operatorname{lcm}(k(2^t), k(p_i^{e_i}))$, so $k(2(r-1)) = \operatorname{lcm}(6.2^{t-2}, k(p_i^{e_i}))$ and therefore $6 | k(2(r-1))$. □

Again we show that these results enable us to reduce the time needed to calculate the Fibonacci length of $F(r,2)$. We use results calculated using the **fpfl** program and a suite of programs created to calculate Wall numbers (the same program used in the G_ℓ case).

r	**fpfl**$(F(r,2))$	time*	$k(2(r-1))$	time*
5	12	170	12	0
7	24	180	24	0
9	24	170	24	0
11	60	180	60	0
13	24	180	24	0
15	48	200	48	0
17	48	200	48	0
19	24	200	24	0
21	60	240	60	0
351	1200	23130	1200	20
371	1140	24210	1140	0
399	66	10300	66	0

$*$ Time is in milliseconds of cpu time.

We finish this chapter with the following note:

Up to now all metacyclic groups mentioned in this chapter, and indeed this thesis, have had even Fibonacci length. We use the following example to illustrate the fact that this is not always so.

Example 4.6 Let G be the group generated by the permutations

$$\alpha = (1,10,19,2,11,20,3,12,21)(4,14,24,5,15,22,6,13,23)(7,18,26,8,16,27,9,17,25),$$

$$\beta = (1,4,7)(2,5,8)(3,6,9)(10,13,16)(11,14,17)(12,15,18)(19,22,25)(20,23,26)(21,24,27),$$

$$\gamma = (1,2,3)(4,5,6)(7,8,9)(10,11,12)(13,14,15)(16,17,18)(19,20,21)(22,23,24)(25,26,27).$$

Now G is a nonabelian group of order 27 with a proper normal subgroup generated by $\alpha^4\beta$ which is the permutation

$$(1,14,25,2,15,26,3,13,27)(4,18,21,5,16,19,6,17,20)(7,10,23,8,11,24,9,12,22).$$

The subgroup $\langle \alpha^4\beta \rangle$ is isomorphic to C_9. By the use of the program **fpfl** it is shown that $LEN_{\{\alpha,\beta,\gamma\}}(G) = 39$. So we have a group G with a cyclic proper normal subgroup, N say, with G/N cyclic. Hence we have shown that a metacyclic group with odd Fibonacci length exists.

This raises the interesting question:

Open questions: Given a metacyclic group G, does there exist a generating set of G with even Fibonacci length?

Chapter 4

The Fibonacci length of direct powers of dihedral groups

1 Introduction

In their 1990 paper Campbell, Doostie and Robertson [19] showed that, when the dihedral group of size $2n$, written D_{2n}, is generated by two elements there is, up to isomorphism, only one Fibonacci orbit of D_{2n}, and thus only one Fibonacci length of D_{2n}. In fact $LEN_{a,b}(D_{2n}) = 6$ for any pair $\{a, b\}$ of generators of D_{2n}. Generating pairs of D_{2n} are of three types

$$a^2 = 1,\ b^2 = 1,\ (ab)^n = 1,$$
$$a^2 = 1,\ b^n = 1,\ (ab)^2 = 1,$$
$$a^n = 1,\ b^2 = 1,\ (ab)^2 = 1.$$

The first type of generating pair gives the Fibonacci orbit $(a, b, ab, bab, b, ba, a, b, \ldots)$.

In this section we investigate if direct products of D_{2n} have constant Fibonacci length. We choose to investigate the natural generating set of D_{2n}^i obtained from

the presentation for D_{2n}

$$\langle\, a, b \mid a^2 = 1, b^n = 1, (ab)^2 = 1 \,\rangle$$

by letting D_{2n}^i be defined by the presentation

$$\begin{aligned}\langle\, a_1,\ b_1,\ a_2,\ b_2,\ \ldots,\ a_i,\ b_i \ \mid\ & a_l^2 = 1, b_l^n = 1, (a_l b_l)^2 = 1, \\ & [a_j, a_k] = [a_j, b_k] = [b_j, b_k] = 1, \\ & 1 \leq l \leq i,\ 1 \leq j < k \leq i \,\rangle.\end{aligned}$$

This method of construction follows that found in [45].

In order to answer this question fully we first investigate the Fibonacci orbit of direct powers of infinite dihedral groups, D_∞^i, defined by the presentation

$$\begin{aligned}\langle\, a_1,\ b_1,\ a_2,\ b_2,\ \ldots,\ a_i,\ b_i \ \mid\ & a_l^2 = 1, (a_l b_l)^2 = 1, \\ & [a_j, a_k] = [a_j, b_k] = [b_j, b_k] = 1, \\ & 1 \leq l \leq i,\ 1 \leq j < k \leq i \,\rangle.\end{aligned}$$

Then using number theory we find when the powers of the exponents in the orbit are divisible by a given positive integer n.

Note: Through out this chapter we will choose to start the Fibonacci orbit with x_1.

Some of the work in this chapter will be published as "On the Fibonacci length of powers of dihedral groups" by C. M. Campbell, P. P. Campbell, H. Doostie and E. F. Robertson, see [17].

2 The Fibonacci orbit of D^i_∞, $i \geq 2$

D^i_∞ has a presentation with $2i$ generators and $2i^2$ relations, namely:

$$D^i_\infty = \langle\, a_1,\ b_1,\ a_2,\ b_2,\ \ldots,\ a_i,\ b_i \ \mid\ a_l^2, (a_l b_l)^2, \\ [a_j, a_k], [a_j, b_k], [b_j, b_k], \\ 1 \leq l \leq i,\ 1 \leq j < k \leq i \,\rangle.$$

The elements of the group defined by the above presentation can be written in the normal form $a_i^{q_i} a_{i-1}^{q_{i-1}} \ldots a_1^{q_1} b_i^{r_i} b_{i-1}^{r_{i-1}} \ldots b_1^{r_1}$ where the q_l are either 0 or 1 and $r_j \in \mathbb{Z}$. Throughout this chapter we will always reduce elements of the Fibonacci orbit to this normal form.

In order to elucidate the main proof of this section we start by considering the Fibonacci type sequence of elements of D^2_∞ as

$$x_1 = a_1, x_2 = b_1, x_3 = a_2, x_4 = b_2, x_n = x_{n-4}x_{n-3}x_{n-2}x_{n-1}, (n \geq 5).$$

We have:

Lemma 2.1 *Every element of the Fibonacci orbit $(x_j)_{j=1}^\infty$ of D^2_∞ given by the presentation*

$$\langle\, a_1, b_1, a_2, b_2 \mid a_1^2, a_2^2, (a_1 b_1)^2, (a_2 b_2)^2, [a_1, a_2], [a_1, b_2], [b_1, a_2], [b_1, b_2] \,\rangle$$

may be represented by:

$$x_j = \begin{cases} a_1, & j \equiv 1, -4 \bmod 10 \\ b_1^{\pm 1}, & j \equiv 2, -3 \bmod 10 \\ a_2 b_1^{\pm 2(j-3)/5}, & j \equiv 3, -2 \bmod 10 \\ b_2^{\pm 1} b_1^{\pm 2(j-4)(j+1)/5^2}, & j \equiv 4, -1 \bmod 10 \\ a_2 a_1 b_2^{\pm 1} b_1^{\pm (2j^2-5^2)/5^2}, & j \equiv 5,\ 0 \bmod 10 \end{cases}$$

where the positive exponent is chosen for the first value of j and the negative exponent is chosen for the second value of j.

Proof. The assertion may be proved by induction on j. We first prove the anchor step of the induction. Since $a_\gamma^i b_\gamma a_\gamma^i = b_\gamma^{-1}$, with $\gamma \in \{1,2\}$ and i odd, we have

$$
\begin{aligned}
x_1 &= a_1, \\
x_2 &= b_1, \\
x_3 &= a_2, \\
x_4 &= b_2, \\
x_5 &= a_2 a_1 b_2 b_1, \\
x_6 &= b_1 a_2 b_2 a_1 b_1 a_2 b_2 = a_1, \\
x_7 &= a_2 b_2 a_1 b_1 a_2 b_2 a_1 = a_1 b_1 a_1 = b_1^{-1}, \\
x_8 &= b_2 a_1 b_1 a_2 b_2 a_1 b_1^{-1} = b_2 a_2 b_2 . a_1 b_1 a_1 b_1^{-1} = a_2 b_1^{-2}, \\
x_9 &= a_1 b_1 a_2 b_2 a_1 b_1^{-1} a_2 b_1^{-2} = a_2 b_2 a_2 . a_1 b_1 a_1 b_1^{-3} = b_2^{-1} b_1^{-4}, \\
x_{10} &= a_1 b_1^{-1} a_2 b_1^{-2} b_2^{-1} b_1^{-4} = a_2 a_1 b_2^{-1} b_1^{-7}.
\end{aligned}
$$

Now let $j \equiv 0 \bmod 10$ and assume that the result holds for all values up to $j+5$, namely

$$
\begin{aligned}
x_{j+1} &= a_1, \\
x_{j+2} &= b_1, \\
x_{j+3} &= a_2 b_1^{2((j+3)-3)/5} = a_2 b_1^{2j/5}, \\
x_{j+4} &= b_2 b_1^{2((j+4)-4)((j+4)+1)/25} = b_2 b_1^{2j(j+5)/25}, \\
x_{j+5} &= a_1 a_2 b_1^{(2(j+5)^2-25)/25} b_2 = a_2 a_1 b_2 b_1^{(2j^2+20j+25)/25}.
\end{aligned}
$$

We now prove that the next ten entries have the required form and thus complete the induction.

$$
x_{j+6} = b_1 a_2 b_1^{2j/5} b_2 b_1^{2j(j+5)/25} a_2 a_1 b_2 b_1^{(2j^2+20j+25)/25}
$$

$$= b_1^{1+2j/5+2j^2/25+10j/25} a_1 b_1^{(2j^2+20j+25)/25} a_2 b_2 a_2 b_2$$
$$= a_1.$$

$$\begin{aligned} x_{j+7} &= a_2 b_1^{2j/5} b_2 b_1^{2j(j+5)/25} a_2 a_1 b_2 b_1^{(2j^2+20j+25)/25} a_1 \\ &= b_1^{2j/5+2j^2/25+10j/25} a_1 b_1^{(2j^2+20j+25)/25} a_1 a_2 b_2 a_2 b_2 \\ &= b_1^{-1}. \end{aligned}$$

$$\begin{aligned} x_{j+8} &= b_2 b_1^{2j(j+5)/25} a_2 a_1 b_2 b_1^{(2j^2+20j+25)/25} a_1 b_1^{-1} \\ &= b_1^{2j^2/25+10j/25} a_1 b_1^{(2j^2+20j+25)/25} a_1 b_1^{-1} b_2 a_2 b_2 \\ &= a_2 b_1^{-2((j+8)-3)/5}. \end{aligned}$$

$$\begin{aligned} x_{j+9} &= a_2 a_1 b_2 b_1^{(2j^2+20j+25)/25} a_1 b_1^{-1} a_2 b_1^{-2((j+8)-3)/5} \\ &= a_1 b_1^{(2j^2+20j+25)/25} a_1 b_1^{-2j/5-3} a_2 b_2 a_2 \\ &= b_2^{-1} b_1^{-2((j+9)-4)((j+9)+1)/25}. \end{aligned}$$

$$\begin{aligned} x_{j+10} &= a_1 b_1^{-1} a_2 b_1^{-2((j+8)-3)/5} b_2^{-1} b_1^{-2((j+9)-4)((j+9)+1)/25} \\ &= a_1 b_1^{-2j/5-7-2j^2/25-15j/25} a_2 b_2^{-1} \\ &= a_2 a_1 b_2^{-1} b_1^{-(2(j+10)^2-25)/25}. \end{aligned}$$

$$\begin{aligned} x_{j+11} &= b_1^{-1} a_2 b_1^{-2((j+8)-3)/5} b_2^{-1} b_1^{-2((j+9)-4)((j+9)+1)/25} a_2 a_1 b_2^{-1} b_1^{-(2j^2+40j+175)/25} \\ &= b_1^{-10j/25-7-2j^2/25-6j/5} a_1 b_1^{-2j^2/25-8j/5-7} a_2 b_2^{-1} a_2 b_2^{-1} \\ &= a_1. \end{aligned}$$

$$\begin{aligned} x_{j+12} &= a_2 b_1^{-2((j+8)-3)/5} b_2^{-1} b_1^{-2((j+9)-4)((j+9)+1)/25} a_2 a_1 b_2^{-1} b_1^{-(2j^2+40j+175)/25} a_1 \\ &= b_1^{-2j/5-2-2j^2/25-6j/5-4} a_1 b_1^{-2j^2/25-8j/5-7} a_1 a_2 b_2^{-1} a_2 b_2^{-1} \\ &= b_1. \end{aligned}$$

$$x_{j+13} = b_2^{-1} b_1^{-2((j+9)-4)((j+9)+1)/25} a_2 a_1 b_2^{-1} b_1^{-(2j^2+40j+175)/25} a_1 b_1$$

$$= b_1^{-2j^2/25-6j/5-4} a_1 b_1^{-2j^2/25-8j/5-7} a_1 b_1 b_2^{-1} a_2 b_2^{-1}$$
$$= a_2 b_1^{2((j+13)-3)/5}.$$

$$x_{j+14} = a_2 a_1 b_2^{-1} b_1^{-(2j^2+40j+175)/25} a_1 b_1 a_2 b_1^{2(j+10)/5}$$
$$= a_1 b_1^{-(2j^2+40j+175)/25} a_1 b_1^{1+2(j+10)/5} a_2 b_2^{-1} a_2$$
$$= b_2 b_1^{2((j+14)-4)((j+14)+1)/25}.$$

$$x_{j+15} = a_1 b_1 a_2 b_1^{2(j+10)/5} b_2 b_1^{2((j+14)-4)((j+14)+1)/25}$$
$$= a_1 b_1^{1+2(j+10)/5+2((j+14)-4)((j+14)+1)/25} a_2 b_2$$
$$= a_2 a_1 b_2 b_1^{(2(j+15)^2-25)/25}.$$ □

In the same manner as the previous case we examine the Fibonacci sequence of D_∞^3 i.e.

$$x_1 = a_1, x_2 = b_1, x_3 = a_2, x_4 = b_2, x_5 = a_3, x_6 = b_3, x_n = \prod_{j=1}^{6} x_{n-7+j}, \ (n \geq 7).$$

Lemma 2.2 *Every element of the Fibonacci orbit $(x_j)_{j=1}^{\infty}$ of D_∞^3 defined by the presentation*

$$\langle\, a_1, b_1, a_2, b_2, a_3, b_3 \ \mid\ a_1^2, a_2^2, a_3^2, (a_1b_1)^2, (a_2b_2)^2, (a_3b_3)^2,$$
$$[a_1, a_2], [a_1, b_2], [a_1, a_3], [a_1, b_3],$$
$$[b_1, a_2], [b_1, b_2], [b_1, a_3], [b_1, b_3],$$
$$[a_2, a_3], [a_2, b_3], [b_2, a_3], [b_2, b_3] \,\rangle$$

may be represented by:

$$x_j = \begin{cases} a_1, & j \equiv 1, -6 \bmod 14 \\ b_1^{\pm 1}, & j \equiv 2, -5 \bmod 14 \\ a_2 b_1^{\pm 2(j-3)/7}, & j \equiv 3, -4 \bmod 14 \\ b_2^{\pm 1} b_1^{\pm 2(j-4)(j+3)/7^2}, & j \equiv 4, -3 \bmod 14 \\ a_3 b_2^{\pm 2(j-5)/7} b_1^{\pm 4(j-5)(j+2)(j+9)/(3\times 7^3)}, & j \equiv 5, -2 \bmod 14 \\ b_3^{\pm 1} b_2^{\pm 2(j+1)(j-6)/7^2} b_1^{\pm 2(j-6)(j+1)(j+8)(j+15)/(3\times 7^4)}, & j \equiv 6, -1 \bmod 14 \\ a_3 a_2 a_1 b_3^{\pm 1} b_2^{\pm (2j^2-7^2)/7^2} b_1^{\pm (2(j/7)^4+8(j/7)^3+4(j/7)^2-8(j/7)-3)/3}, & j \equiv 7,\ 0 \bmod 14 \end{cases}$$

where the positive exponent is chosen for the first value of j and the negative exponent is chosen for the second value of j.

Proof. See Appendix B for proof. □

We now seek to generalize the above to obtain a normal form for the Fibonacci orbit of D_∞^i, $i \geq 2$. We will need the following result in our calculations.

Lemma 2.3 *For $n \geq 3$ the following polynomial identity holds:*

$$\begin{aligned} 2 + \sum_{j=3}^{n-1} \frac{2^{j-2}}{(j-2)!} m(m+1)(m+2)\dots(m+j-3) \\ + \sum_{j=3}^{n} \frac{2^{j-2}}{(j-2)!} (m-1)m(m+1)\dots(m+j-4) \\ = \frac{2^{n-2}}{(n-2)!} m(m+1)(m+2)\dots(m+n-3) \end{aligned}$$

with the convention that when $n = 3$, the first term in the first summation on the left hand side is zero.

Proof. We use induction on n.

When $n = 3$ the result holds since $2 + 0 + \frac{2}{1!}(m-1) = 2m$, i.e. $\frac{2}{1!}m = 2m$.

When $n = 4$ the result also holds since

$$2 + \frac{2}{1!}m + \frac{2}{1!}(m-1) + \frac{2^2}{2!}(m-1)m = 2m(m+1), \text{ i.e. } \frac{2^2}{2!}m(m+1) = 2m(m+1).$$

Now assume that the result holds for all values less than n. Then

$$2 + \sum_{j=3}^{n-1} \frac{2^{j-2}}{(j-2)!}m(m+1)\dots(m+j-3) + \sum_{j=3}^{n} \frac{2^{j-2}}{(j-2)!}(m-1)m\dots(m+j-4)$$

$$= 2 + \sum_{j=3}^{n-2} \frac{2^{j-2}}{(j-2)!}m(m+1)\dots(m+j-3) + \sum_{j=3}^{n-1} \frac{2^{j-2}}{(j-2)!}(m-1)m\dots(m+j-4)$$

$$+ \frac{2^{n-3}}{(n-3)!}m(m+1)\dots(m+n-4) + \frac{2^{n-2}}{(n-2)!}(m-1)m\dots(m+n-4).$$

By the inductive hypothesis this is equal to

$$\frac{2^{n-3}}{(n-3)!}m(m+1)\dots(m+n-4) + \frac{2^{n-3}}{(n-3)!}m(m+1)\dots(m+n-4)$$

$$+ \frac{2^{n-2}}{(n-2)!}(m-1)m\dots(m+n-4)$$

$$= \frac{2^{n-2}}{(n-3)!}m(m+1)\dots(m+n-4) + \frac{2^{n-2}}{(n-2)!}(m-1)m\dots(m+n-4)$$

$$= \frac{2^{n-2}}{(n-2)!}m(m+1)\dots(m+n-3)$$

as required. □

Now we make the following observations about the Fibonacci orbits $(x_j)_{j=1}^{\infty}$ of the groups $D_{\infty}^{i} = \langle a_1, b_1, a_2, b_2, \dots, a_i, b_i \rangle$ (where $i \in \mathbb{N}$).

Lemma 2.4 *The exponent of b_l in x_j is zero if $j \equiv 1, 2, \dots, 2l-1 \bmod (2i+1)$, where $l \in \{1, 2, \dots, i\}$.*

Proof. This is easy to see if we look at the 'structure' of the entries of the Fibonacci orbit $(x_j)_{j=1}^{\infty}$ of D_{∞}^{i}. For $j \in \{1, 2, \ldots, 2i\}$ we have

$$x_j = \begin{cases} a_{(j+1)/2}, & \text{if } j \text{ is odd,} \\ b_{j/2}, & \text{if } j \text{ is even,} \end{cases}$$

and

$$x_{2i+1} = \prod_{d=1}^{2i} x_d.$$

Now it is easy to see that the next term of the Fibonacci orbit to contain an a_l will be

$$x_{2l+2i} = \prod_{d=2l}^{2l+2i-1} x_d.$$

Likewise the next b_l occurs in the next entry of the Fibonacci orbit, namely:

$$x_{2l+2i+1} = \prod_{d=2l+1}^{2l+2i} x_d.$$

The final stage of the induction follows by using an argument analogous to that above. □

Remark 2.5 It can easily be shown that the exponents of b_l can be calculated once one knows the exponents of b_1 since the exponents of b_l 'lag' behind the exponents of b_1. This holds because all b_l's initially have exponent one and from Lemma 2.4 above it can be seen when the exponents of b_l are nonzero. As an example of this 'lag' see the D_{∞}^{3} case where, when $j \equiv 3 \bmod 14$, the power of b_1 is $2(j-3)/7$, and when $j \equiv 5 \bmod 14$, the power of b_2 is $2(j-5)/7$.

These results are best illustrated by looking at the D_{∞}^{3} case (given separately in Lemma 2.2). It can be used as an example in the following proof to elucidate concepts. In this case the orbit is

$$\begin{aligned} Z = \; & (a_1, b_1, a_2, b_2, a_3, b_3, a_3a_2a_1b_3b_2b_1, \\ & a_1, b_1^{-1}, a_2b_1^{-2}, b_2^{-1}b_1^{-4}, a_3b_2^{-2}b_1^{-4}, b_3^{-1}b_2^{-4}b_1^{-8}, a_3a_2a_1b_3^{-1}b_2^{-7}b_1^{-19}, \\ & a_1, b_1, \ldots). \end{aligned}$$

So the Fibonacci orbit behaves as if it is in 'layers' of length $2i+1$ where in alternate layers the exponents of b_l are all positive and all negative. Since one layer's 'structure' depends only on the previous layer, a proof by induction will only need the first layer to be proved to anchor the induction. Also we note here that it is unnecessary to know the general form of the $k(2i+1)th$ entry ($k \in \mathbb{N}$) in the Fibonacci orbit since this will always be the product of all the previous terms in its layer and so this entry has a known shape, namely $a_i a_{i-1} \ldots a_1 b_i^{w_i} b_{i-1}^{w_{i-1}} \ldots b_1^{w_1}$ where w_l is the sum of the exponents of b_l in the layer.

We are now ready to give the main result of this section.

Proposition 2.6 *The exponents of b_1 in the Fibonacci orbit $(x_j)_{j=1}^{\infty}$ of D_∞^i are given in the table below*

$$\begin{array}{ll} 0, & j \equiv 1,\ 2i+2 \bmod (4i+2) \\ \pm 1, & j \equiv 2,\ 2i+3 \bmod (4i+2) \\ \pm A_n(\prod_{d=0}^{n-3}(j-n+d(2i+1)))/(2i+1)^{n-2}, & j \equiv n,\ 2i+1+n \bmod (4i+2) \\ \sum_{d=j-2i}^{j-1} z_d, & j \equiv 2i+1,\ 0 \bmod (4i+2) \end{array}$$

where $A_n = 2^{n-2}/(n-2)!$, z_r is the exponent of b_1 in x_r, $n \equiv j \bmod (2i+1)$ so $3 \leq n \leq 2i$ and the positive forms of elements in the orbit are chosen if $1 \leq j \bmod (4i+2) \leq 2i+1$; otherwise choose the (second) negative forms.

Proof. Let the exponent of b_1 in the x_r entry of the Fibonacci orbit be z_r. Assume that the result is true for all values of j such that $1 \leq j < k$. There are several cases to examine:

- Case 1. $k \equiv 1, 2i+2 \bmod (4i+2)$

In this case we have

$$\underline{b_1^{z_{k-2i}+\ldots+z_{k-2}} a_1 b_1^{z_{k-2i}+\ldots+z_{k-2}}} = a_1.$$

- Case 2. $k \equiv 2, 2i+3 \bmod (4i+2)$

Here we have

$$\underline{b_1^{z_{k-2i}+\ldots+z_{k-3}} a_1 b_1^{z_{k-2i-2}+\ldots+z_{k-3}}} a_1 = \underline{a_1 b_1^{0+z_{k-2i-1}} a_1} = b_1^{-z_{k-2i-1}} = b_1^{\pm 1}.$$

- Case 3. $k \equiv n, 2i+n+1 \bmod (4i+2)$, $3 \leq n \leq 2i+1$

When we are trying to calculate the exponent of b_1 for the kth entry in the Fibonacci orbit we need only concentrate on the terms in a_1 and b_1. The exponent of b_1 and a_1 in the kth entry in the Fibonacci orbit is

$$(\prod_{l=k-2i}^{x-1} b_1^{z_l})(a_1 \prod_{l=x-2i}^{x-1} b_1^{z_l}) a_1 (\prod_{l=x+1}^{k-1} b_1^{z_l})$$

where $x = (2i+1)\lfloor k/(2i+1) \rfloor$. (Note the first bracket is from the layer below that of x_k, the second bracket is the last entry in the lower layer). The above sum can be simplified using the group relations as follows

$$\underline{(\prod_{l=k-2i}^{x-1} b_1^{z_l})(a_1 \prod_{l=x-2i}^{x-1} b_1^{z_l}) a_1} (\prod_{l=x+1}^{k-1} b_1^{z_l}) = \underline{a_1 (\prod_{l=x-2i}^{k-2i-1} b_1^{z_l}) a_1} (\prod_{l=x+1}^{k-1} b_1^{z_l}),$$

$$= (\prod_{l=x-2i}^{k-2i-1} b_1^{-z_l})(\prod_{l=x+1}^{k-1} b_1^{z_1}).$$

Thus the exponent of b_1 is given by

$$\sum_{l=x+1}^{k-1} z_l - \sum_{l=x-2i}^{k-2i-1} z_l$$

$$= \pm(0+1+A_3((x+3)-3)/(2i+1)+\ldots$$

$$+A_{k-x-1}\left[\prod_{d=0}^{k-x-4}((k-1)-(k-x-1)+d(2i+1))\right]/(2i+1)^{k-x-3})$$

$$-(\mp(0+1+A_3((x-2i+2)-3)/(2i+1)+\ldots$$

$$+A_{k-x}\left[\prod_{d=0}^{k-x-3}((k-2i-1)-(k-x)+d(2i+1))\right]/(2i+1)^{k-x-2})$$

So we want to show that

$$2+\sum_{l=3}^{n-1}\frac{2^{l-2}}{(l-2)!}m(m+1)\ldots(m+l-3)+\sum_{l=3}^{n}\frac{2^{l-2}}{(l-2)!}(m-1)m(m+1)\ldots(m+l-4)$$

$$=\frac{2^{n-2}}{(n-2)!}m(m+1)\ldots(m+n-3)$$

where $n \equiv k \bmod (2i+1)$, $m = \lfloor k/(2i+1) \rfloor$ and $2 < n < 2i+1$ and $\sum_{l=3}^{n-1}(2^{l-2}m(m+1)\ldots(m+l-3)/(l-2)!)$ is zero if $n = 3$. Now the result follows by using Lemma 2.3.

- Case 4. $k \equiv 2i+1, 0 \bmod (4i+2)$

Here there is nothing to prove. □

We will illustrate this result via an example:

Example 2.7 We will calculate the power of b_1 in the group D_∞^3 using the above proposition and compare it to the results proved earlier. We know that $i = 3$ so

$2i+1=7$. The powers of b_1 in D_∞^3 are z_j where:

$$z_j = \begin{cases} 0, & j \equiv 1,\ 8 \bmod 14 \\ \pm 1, & j \equiv 2,\ 9 \bmod 14 \\ \pm 2(j-3)/7, & j \equiv 3,\ 10 \bmod 14 \\ \pm 2(j-4)(j+3)/7^2, & j \equiv 4,\ 11 \bmod 14 \\ \pm 4(j-5)(j+2)(j+9)/3(7^3), & j \equiv 5,\ 12 \bmod 14 \\ \pm 2(j-6)(j+1)(j+8)(j+15)/3(7^4), & j \equiv 6,\ 13 \bmod 14 \\ \pm \sum_{d=j-2i}^{j-1} z_d, & j \equiv 7,\ 0 \bmod 14 \end{cases}$$

So the results due to the proposition agree with those calculated in Lemma 2.2.

3 The Fibonacci length of D_{2m}^i, $i \geq 2$

In order to give an expression for the Fibonacci length of D_{2m}^i, $i \geq 2$, we require the following definitions and lemmas.

Definition 3.1 In D_{2m}^i let $MinLEN(D_{2m}^i) = 2m(2i+1)/(4,m)$.

Remark 3.2 We note here that when $n = LEN(D_{2m}^i)$ we have $x_{n+1} = a_1$, $x_{n+2} = b_1, x_{n+3} = a_2, \ldots, x_{n+2i} = b_i$ so we need the exponent of b_1 in the entries $x_{n+1}, x_{n+3}, \ldots, x_{n+2i}$ to be a multiple of the order of b_1 ($|b_1| = m$ in D_{2m}^i), i.e. $z_{n+1} = y_1 m, z_{n+3} = y_3 m, \ldots, z_{n+2i} = y_{2i} m$, where $y_1, y_3, \ldots, y_{2i} \in \mathbb{Z}$. Also note that, using Proposition 2.6, if we let $l = MinLEN(D_{2m}^i) = 2m(2i+1)/(4,m)$ and $3 \leq n \leq 2i$ we have

$$z_{l+n} = \frac{2^{n-2} l(l+(2i+1)) \ldots (l+(n-3)(2i+1))}{(n-2)!(2i+1)^{n-2}}.$$

So increasing m will not alter the denominator of z_{l+n} given above.

Lemma 3.3 *In D_{2m}^i, $i \geq 2$, $MinLEN(D_{2m}^i)$ divides $LEN(D_{2m}^i)$, and the quotient $LEN(D_{2m}^i)/MinLEN(D_{2m}^i)$ only involves odd prime divisors of m.*

Proof. We first note that $MinLEN(D_{2m}^i)$ is the smallest possible Fibonacci length since by Proposition 2.6 we must have $(4i+2) \mid LEN(D_{2m}^i)$ and, from the third entry in the Fibonacci orbit of D_{2m}^i, we also have $m \mid (2LEN(D_{2m}^i)/(2i+1))$. Thus $MinLEN(D_{2m}^i)$ divides $LEN(D_{2m}^i)$.

Now let $l = MinLEN(D_{2m}^i)$. By Proposition 2.6 for $3 \leq n \leq 2i$ we have

$$z_{l+n} = \frac{2^{n-2}l(l+(2i+1))\ldots(l+(n-3)(2i+1))}{(n-2)!(2i+1)^{n-2}}.$$

If $\bar{l} = l/(2i+1) = 2m/(4,m)$ the above becomes

$$z_{l+n} = \frac{2^{n-2}\bar{l}(\bar{l}+1)\ldots(\bar{l}+(n-3))}{(n-2)!}.$$

Now z_{l+n} is obviously an integer. Since z_{l+n} is the power of b_1 in the $(l+n)th$ entry of the Fibonacci orbit we require that m, $m = |b_1|$, divides $z_{LEN(D_{2m}^i)+n}$, with $3 \leq n \leq 2i$. It may occur that, for a given m and i, $m \not| z_{l+n}$ because powers of primes from the factorization of m that also occur in the numerator of z_{l+n} may be factored out by the $(n-2)!$ denominator. Let these 'missing' primes be $p_j^{\alpha_j}\ldots p_r^{\alpha_r}$. Now multiplying l by a factor q less than $p_j^{\alpha_j}\ldots p_r^{\alpha_r}$ will not be sufficient. For m will not divide z_{ql+n} since the denominator $(n-2)!$ will be the same as in the z_{l+n} case and the numerator will still be a product of 2^{n-2} and $n-2$ consecutive integers but this time starting at $2qm/(4,m)$. Thus $(n-2)!$ will still factor out $p_j^{\alpha_j}\ldots p_r^{\alpha_r}$ and since q is less than $p_j^{\alpha_j}\ldots p_r^{\alpha_r}$ we still have $m \not| z_{ql+n}$. If we let $q = p_j^{\alpha_j}\ldots p_r^{\alpha_r}$ then we will have $m | z_{ql+n}$. □

Corollary 3.4 *If $j = LEN(D_{2m}^i)$, then*

$$z_{j+n} = 2^{n-2}\begin{pmatrix} \bar{j}+n-3 \\ n-2 \end{pmatrix},$$

where $\bar{j} = j/(2i+1)$ and $3 \leq n \leq 2i$.

Proof. We will use the notation from the statement of the corollary. That the quotient $LEN(D^i_{2m})/(2i+1)$ is an integer follows from the proof of the previous lemma. Using Proposition 2.6 we see that

$$\begin{aligned} z_{j+n} &= \frac{2^{n-2}j(j+(2i+1))\ldots(j+(n-3)(2i+1))}{(n-2)!(2i+1)^{n-2}} \\ &= \frac{2^{n-2}\overline{j}(\overline{j}+1)\ldots(\overline{j}+(n-3))}{(n-2)!}. \end{aligned}$$

Now

$$\begin{aligned} 2^{n-2}\begin{pmatrix} \overline{j}+n-3 \\ n-2 \end{pmatrix} &= 2^{n-2}(\overline{j}+n-3)!/((\overline{j}+n-3-n+2)!(n-2)!) \\ &= 2^{n-2}(\overline{j}+n-3)!/((\overline{j}-1)!(n-2)!) \\ &= 2^{n-2}(\overline{j}+n-3)\ldots(\overline{j}+1)(\overline{j})/(n-2)! \\ &= z_{j+n} \end{aligned}$$

as required. □

Thus this section is concerned about calculating when a certain binomial coefficient is divisible by a given number. This is an old open problem and is closely linked to other open problems from number theory, see [34], [35], [37] and [61].

Unfortunately the value $MinLEN(D^i_{2m})$ is not always equal to the Fibonacci length of D^i_{2m} as the next examples will show.

Example 3.5 Let $\overline{l} = MinLEN(D^i_{2m})/(2i+1) = 2m/(4,m)$ with $i=3$, $m=5$. This gives $\overline{l}=10$ and $3 \leq n \leq 6$. So using

$$z_{l+n} = \frac{2^{n-2}\overline{l}(\overline{l}+1)\ldots(\overline{l}+(n-3))}{(n-2)!},$$

we obtain the following results

$$\begin{aligned}
z_{MinLEN(D^3_{2(5)})+3} &= \frac{2(10)}{(1)} = 20 \\
z_{MinLEN(D^3_{2(5)})+4} &= \frac{2^2(10)(11)}{(1)(2)} = 220 \\
z_{MinLEN(D^3_{2(5)})+5} &= \frac{2^3(10)(11)(12)}{(1)(2)(3)} = 1760 \\
z_{MinLEN(D^3_{2(5)})+6} &= \frac{2^4(10)(11)(12)(13)}{(1)(2)(3)(4)} = 11440
\end{aligned}$$

All the above elements of the Fibonacci orbit of $D^3_{2(5)}$ are divisible by 5 so in this case $LEN(D^3_{2(5)}) = MinLEN(D^3_{2(5)})$ as we must have the powers of b_j, $3 \leq j \leq 2i$, a multiple of the order of b_1, 5 in this case, and $MinLEN(D^3_{2(5)})$ is the minimal possible value.

We now present an example where $MinLEN(D^i_{2m}) \neq LEN(D^i_{2m})$.

Example 3.6 Let $i = 4, m = 5$ so $3 \leq n \leq 8$. As above, we have

$$\begin{aligned}
z_{MinLEN(D^3_{2(5)})+3} &= \frac{2(10)}{(1)} = 20 \\
z_{MinLEN(D^3_{2(5)})+4} &= \frac{2^2(10)(11)}{(1)(2)} = 220 \\
z_{MinLEN(D^3_{2(5)})+5} &= \frac{2^3(10)(11)(12)}{(1)(2)(3)} = 1760 \\
z_{MinLEN(D^3_{2(5)})+6} &= \frac{2^4(10)(11)(12)(13)}{(1)(2)(3)(4)} = 11440 \\
z_{MinLEN(D^3_{2(5)})+7} &= \frac{2^5(10)(11)(12)(13)(14)}{(1)(2)(3)(4)(5)} = 64064 \\
z_{MinLEN(D^3_{2(5)})+8} &= \frac{2^6(10)(11)(12)(13)(14)(15)}{(1)(2)(3)(4)(5)(6)} = 320320
\end{aligned}$$

Now all the above are divisible by 5 except the $z_{MinLEN(D^3_{2(5)})+7}$ value, so in this case $LEN(D^4_{2(5)}) \neq MinLEN(D^4_{2(5)})$.

So with this example in mind we introduce the following definition.

Definition 3.7 Let $\pi_{m,i} \in \mathbb{N}$ be defined as satisfying the equation $LEN(D^i_{2m}) = \pi_{m,i} MinLEN(D^i_{2m})$.

We now give a property of $\pi_{m,i}$ that will be used in a later lemma.

Lemma 3.8 *For any fixed m the sequence $(\pi_{m,i})_{i=2}^{\infty}$ is monotonically increasing.*

Proof. Let $l = LEN(D^i_{2m}) = 2m\pi_{m,i}(2i+1)/(4,m)$ and $\bar{l} = l/(2i+1)$. From Proposition 2.6 for $3 \leq n \leq 2i$ we have

$$\begin{aligned} z_{l+n} &= \frac{2^{n-2}\bar{l}(\bar{l}+1)\ldots(\bar{l}+(n-3))}{(n-2)!} \\ &= \frac{2^{n-2}(2m\pi_{m,i}/(4,m))((2m\pi_{m,i}/(4,m))+1)\ldots((2m\pi_{m,i}/(4,m))+(n-3))}{(n-2)!}. \end{aligned}$$

As i increases, and m remains constant, the number of entries in the layers of the Fibonacci orbit increases as does $(2i-2)!$. This gives the possibility that the number and size of primes in the prime decomposition of $(2i-2)!$ will increase and as a consequence so will $\pi_{m,i}$. Note if $\pi_{m,i+1} \not> \pi_{m,i}$ then since $(2i)! > (2i-2)!$, $\pi_{m,i+1} = \pi_{m,i}$. □

Now we show a multiplicative property of $\pi_{m,i}$.

Lemma 3.9 *For $m, n \in \mathbb{N}$, $(m,n) = 1$ and $i \geq 2$, $\pi_{mn,i} = \pi_{m,i}\pi_{n,i}$.*

Proof. Let $m = p_1^{\alpha_1}\ldots p_r^{\alpha_r}$ and $n = q_1^{\beta_1}\ldots q_t^{\beta_t}$ where $(m,n) = 1$ and both p's and q's are prime numbers. For $3 \leq k \leq 2i$ using Lemma 3.3 we obtain

$$\begin{aligned} z_{MinLEN(D^i_{2m})+k} &= \frac{2^{k-2}(2m/(4,m))(2m/(4,m)+1)\ldots(2m/(4,m)+(k-3))}{(k-2)!}, \\ z_{MinLEN(D^i_{2n})+k} &= \frac{2^{k-2}(2n/(4,n))(2n/(4,n)+1)\ldots(2n/(4,n)+(k-3))}{(k-2)!}, \\ z_{MinLEN(D^i_{2mn})+k} &= \frac{2^{k-2}(2mn/(4,mn))(2mn/(4,mn)+1)\ldots(2mn/(4,mn)+(k-3))}{(k-2)!}. \end{aligned}$$

If, for a certain l, $3 \leq l \leq 2i$, $m \not| z_{MinLEN(D^i_{2m})+l}$ then the denominator $(l-2)!$ has factored out some p_i's. If for a certain j, $3 \leq j \leq 2i$, $n \not| z_{MinLEN(D^i_{2n})+j}$ then the denominator $(j-2)!$ has factored out some q_i's. It is now easy to see that the primes needed to be multiplied back so that $m|z_{MinLEN(D^i_{2m})+k}$, $n|z_{MinLEN(D^i_{2n})+k}$ and $mn|z_{MinLEN(D^i_{2mn})+k}$ i.e. $\pi_{m,i}$, $\pi_{n,i}$ and $\pi_{mn,i}$ resp. will satisfy $\pi_{mn,i} = \pi_{m,i}\pi_{n,i}$. □

Lemma 3.10 *If p is an odd prime and $\alpha \in \mathbb{N}$ then $\pi_{p^\alpha,i} = \pi_{p,i}$.*

Proof. Here we use induction on i.

When $i = 2$, letting $l = MinLEN(D^i_{2p}) = 2p(2i+1)/(4,p) = 10p$ and using Proposition 2.6 we obtain

$$\begin{aligned} z_{l+3} &= 2(2p), \\ z_{l+4} &= 2(2p)(2p+1). \end{aligned}$$

Both z_{l+3} and z_{l+4} are divisible by p and so $l = MinLEN(D^i_{2p}) = LEN(D^i_{2p})$ and $\pi_{p,2} = 1$. Using an analogous argument we see that $\pi_{p^\alpha,2} = 1$.

Now assume that $\pi_{p^\alpha,i} = \pi_{p,i}$ for all $i \leq \mu$. We examine the case $\mu+1$. By Lemma 3.8 there are three possibilities:

- Case 1: $\pi_{p^\alpha,\mu+1} = \pi_{p^\alpha,\mu}$ and $\pi_{p,\mu+1} = \pi_{p,\mu}$

  Here there is nothing to prove.

- Case 2: $\pi_{p^\alpha,\mu+1} > \pi_{p^\alpha,\mu}$

Let $l = LEN(D^{\mu}_{2p^{\alpha}})$, $3 \leq n \leq 2\mu$, $\bar{l} = l/(2\mu+1) = 2p^{\alpha}\pi_{p^{\alpha},\mu}/(4, p^{\alpha}) = 2p^{\alpha}\pi_{p^{\alpha},\mu}$ so the power of b_1 in the Fibonacci orbit is given by

$$z_{l+n} = \frac{2^{n-2}2p^{\alpha}\pi_{p^{\alpha},\mu}(2p^{\alpha}\pi_{p^{\alpha},\mu}+1)\ldots(2p^{\alpha}\pi_{p^{\alpha},\mu}+n-3)}{(n-2)!}.$$

We must have $p^{\alpha}|z_{l+n}$ (since $|b_1| = p^{\alpha}$).

Now consider what happens in the $D^{\mu+1}_{2p^{\alpha}}$ case. Keeping l to be the Fibonacci length of $D^{\mu}_{2p^{\alpha}}$ but letting $3 \leq n \leq 2\mu+2$, as above we obtain

$$z_{l+n} = \frac{2^{n-2}2p^{\alpha}\pi_{p^{\alpha},\mu}(2p^{\alpha}\pi_{p^{\alpha},\mu}+1)\ldots(2p^{\alpha}\pi_{p^{\alpha},\mu}+n-3)}{(n-2)!},$$

and since we require $\pi_{p^{\alpha},\mu+1} > \pi_{p^{\alpha},\mu}$ we have $p^{\alpha} \not| z_{l+n}$ for some n, $3 \leq n \leq 2\mu+2$. For n in the range $3 \leq n \leq 2\mu$ we have $p^{\alpha}|z_{l+n}$ (this is just the previous μ case), so p^{α} does not divide one or both of z_{l+n}, $n = 2\mu+1$ or $2\mu+2$. This means that $(2\mu)!$ contains a power of p, p^{γ} say. Thus $\pi_{p^{\alpha},\mu+1} = p^{\gamma}\pi_{p^{\alpha},\mu}$.

We now examine the powers of b_1 in the Fibonacci orbit of $D^{\mu+1}_{2p}$ and letting $l = LEN(D^{\mu}_{2p})$, $3 \leq n \leq 2\mu+2$ gives

$$z_{l+n} = \frac{2^{n-2}2p\pi_{p,\mu}(2p\pi_{p,\mu}+1)\ldots(2p\pi_{p,\mu}+n-3)}{(n-2)!}.$$

For $3 \leq n \leq 2\mu$, $p|z_{l+n}$ but for either $n = 2\mu+1$ or $2\mu+2$ we introduce a factor of $(2\mu-1)(2\mu)$ in the denominator, as in the $D^{\mu+1}_{2p^{\alpha}}$ case, which contains p^{γ}. So since, by the inductive hypothesis, $\pi_{p,\mu} = \pi_{p^{\alpha},\mu}$ and the interval $[2p^{\alpha}\pi_{p^{\alpha},\mu}, 2p^{\alpha}\pi_{p^{\alpha},\mu} + n-3]$ contains the same number of integers as the interval $[2p\pi_{p,\mu}, 2p\pi_{p,\mu}+n-3]$ it follows that $\pi_{p,\mu+1} = p^{\gamma}\pi_{p,\mu}$.

By the inductive hypothesis we know that $\pi_{p^{\alpha},\mu} = \pi_{p,\mu}$. Thus $\pi_{p,\mu+1} = p^{\gamma}\pi_{p,\mu} = p^{\gamma}\pi_{p^{\alpha},\mu} = \pi_{p^{\alpha},\mu+1}$.

- Case 3: $\pi_{p,\mu+1} > \pi_{p,\mu}$

Using an analogous argument as the above we see that in this case $\pi_{p^\alpha,\mu+1} = \pi_{p,\mu+1}$. □

We now deal with powers of the prime 2.

Definition 3.11 The *exponent* of the prime p in the number $n = ap^\alpha$, where $(a,p) = 1$ is equal to α.

First we will need some results giving a bound for the exponent of a given prime p in $n!$.

Lemma 3.12 *The exponent of the prime p in $n!$ is given by*

$$\sum_{i>0} \lfloor \frac{n}{p^i} \rfloor$$

Proof. This is a well known result, see [37]. □

We now find a relationship between n and the exponent of p in $n!$. The proof will fall into three distinct cases depending on the three possible base p representations of two consecutive integers.

Lemma 3.13 *Let $n \geq 1$ be a fixed integer. Then the exponent of the prime p in $n!$ is less than n i.e.*

$$n > \sum_{i>0} \lfloor \frac{n}{p^i} \rfloor.$$

Proof. Fix an arbitrary prime p. We will use induction on n.

If $n = 1$ then the result is true.

Now let the result hold for any integer less than or equal to k. Write

$$k = a_\alpha p^\alpha + a_{\alpha-1}p^{\alpha-1} + \ldots + a_2p^2 + a_1p + a_0$$

where $0 \leq a_i < p$ for all $i \in \{0, 1, \ldots, \alpha\}$. There are three possibilities for $k+1$, namely:

$$\begin{aligned}
(1)\ k+1 &= a_\alpha p^\alpha + a_{\alpha-1}p^{\alpha-1} + \ldots + a_2 p^2 + a_1 p + a_0 + 1, \\
(2)\ k+1 &= a'_\alpha p^\alpha + a'_{\alpha-1}p^{\alpha-1} + \ldots + a'_2 p^2 + a'_1 p, \\
(3)\ k+1 &= p^{\alpha+1},
\end{aligned}$$

where $0 \leq a_i < p$ for all $i \in \{1, \ldots, \alpha\}$, $0 \leq a_0 < p-1$ and $0 \leq a'_i < p$ with $a'_i = a_i$ or $a_1 + 1$. We examine each case individually

- $k+1 = a_\alpha p^\alpha + a_{\alpha-1}p^{\alpha-1} + \ldots + a_2 p^2 + a_1 p + a_0 + 1$

  This possibility gives

$$k+1 > k > \sum_{i>0} \lfloor \frac{k}{p^i} \rfloor = \sum_{i>0} \lfloor \frac{k+1}{p^i} \rfloor.$$

- $k+1 = a'_\alpha p^\alpha + a'_{\alpha-1}p^{\alpha-1} + \ldots + a'_2 p^2 + a'_1 p$

  Using the fact that $a'_i/p^j \leq (p-1)/p^j$ and $(p-1)\sum_{i=0}^{n} 1/p^i = (p^{n+1} - p)/p^{n+1} < 1$ we have:

$$\begin{aligned}
\lfloor \frac{k+1}{p} \rfloor &= a'_\alpha p^{\alpha-1} + a'_{\alpha-1}p^{\alpha-2} + \ldots + a'_2 p + a'_1, \\
\lfloor \frac{k+1}{p^2} \rfloor &= a'_\alpha p^{\alpha-2} + a'_{\alpha-1}p^{\alpha-3} + \ldots + a'_2, \\
&\vdots \quad\quad \vdots \\
\lfloor \frac{k+1}{p^\alpha} \rfloor &= a'_\alpha.
\end{aligned}$$

Considering the sum of each individual column we obtain

$$\begin{aligned}\sum_{i>0}\lfloor\frac{k+1}{p^i}\rfloor &= a'_\alpha(p^{\alpha-1}+p^{\alpha-2}+\ldots+1)\\ &\quad +a'_{\alpha-1}(p^{\alpha-2}+p^{\alpha-3}+\ldots+1)\\ &\quad +\ldots+a'_1(1)\\ \\ &= a'_\alpha(\frac{p^\alpha-1}{p-1})+a'_{\alpha-1}(\frac{p^{\alpha-1}-1}{p-1})+\ldots+a'_1(\frac{p-1}{p-1}),\\ &= \frac{1}{p-1}(a'_\alpha(p^\alpha-1)+a'_{\alpha-1}(p^{\alpha-1}-1)+\ldots+a'_1(p-1)),\\ &= \frac{1}{p-1}(k+1-(a'_\alpha+a'_{\alpha-1}+\ldots+a'_1))<k+1.\end{aligned}$$

- $k+1=p^{\alpha+1}$

  This last possibility gives us

$$\begin{aligned}\sum_{i>0}\lfloor\frac{k+1}{p^i}\rfloor &= \sum_{i>0}\lfloor\frac{p^{\alpha+1}}{p^i}\rfloor\\ &= \sum_{i=0}^{\alpha}p^i\\ &= (p^{\alpha+1}-1)/(p-1)\\ &< p^{\alpha+1}=k+1.\end{aligned}$$

  So the result holds.

  Alternatively for $p>2$

$$\begin{aligned}\sum_{i>0}\lfloor\frac{n}{p^i}\rfloor &= \lfloor\frac{n}{p}\rfloor+\lfloor\frac{n}{p^2}\rfloor+\lfloor\frac{n}{p^3}\rfloor+\ldots\\ &\leq \lfloor\frac{n}{p}+\frac{n}{p^2}+\frac{n}{p^3}+\ldots\rfloor\\ &= \lfloor n(\frac{1}{p-1})\rfloor\\ &< n.\end{aligned}$$

□

As a direct consequence of the above we obtain

Corollary 3.14 *For n a non-negative positive integer and p a prime,*

$$\frac{n!}{p^n} \in \mathbb{Q} \setminus \mathbb{Z}.$$

Proof. Let $n! = p^k x$ where p is an odd prime, $k < n$ and $(x, p) = 1$. From Lemma 3.13 we have $n!/p^n = x/p^{n-k} \in \mathbb{Q} \setminus \mathbb{Z}$ as required. □

We will require the following result.

Corollary 3.15

$$\frac{2^n}{n!} = \frac{2^i}{p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}}$$

where p_j are distinct odd primes, $\alpha_j \in \mathbb{N}$ and $i \leq n$.

Proof. By the proof of Corollary 3.14 and letting $p = 2$ we have $n!/p^n = x/p^{n-k}$ where $n! = p^k x$, $k < n$ and $(2, x) = 1$. Inverting this, writing x in its prime decomposition and letting $i = n - k$ gives the desired result. □

Lemma 3.16 *For any $\beta \in \mathbb{N}$, $\pi_{2^\beta, i} = 1$.*

Proof. The lemma holds since if we examine the powers of b_1 in the Fibonacci orbit of $D^i_{2(2^\beta)}$ we have, for $l = MinLEN(D^i_{2(2^\beta)}) = 2(2i+1)(2^\beta/(4, 2^\beta))$, $i \geq 2$, $3 \leq n \leq 2i$,

$$z_{l+n} = \frac{2^{n-2} 2(2^\beta/(4, 2^\beta))(2(2^\beta/(4, 2^\beta)) + 1) \dots (2(2^\beta/(4, 2^\beta)) + n - 3)}{(n-2)!}.$$

By Lemma 3.13, $2^{n-2}/(n-2)! = 2^t/x$ with $(2, x) = 1$ and $t \geq 1$,

$$z_{l+n} = \frac{2^\beta 2^t (2(2^\beta/(4, 2^\beta)) + 1) \dots (2(2^\beta/(4, 2^\beta)) + n - 3)}{x}$$

or

$$z_{l+n} = \frac{2^\beta 2^{t-1} (2(2^\beta/(4, 2^\beta)) + 1) \dots (2(2^\beta/(4, 2^\beta)) + n - 3)}{x}$$

and so $2^{\beta}|z_{l+n}$. □

Definition 3.17 For $i \geq 2$, let $m = 2^{\alpha_0}p_1^{\alpha_1}\dots p_k^{\alpha_k}$ where p_l are distinct odd primes, and let $t_l = \lfloor \log_{p_l}(2i-3) \rfloor$. Define $\Phi_{m,i} = p_1^{t_1}\dots p_k^{t_k}$, and for all $\alpha \geq 1$, $\Phi_{2^{\alpha},i} = 1$.

Remark 3.18 The definition of $\Phi_{m,i}$ is equivalent to finding for $m = 2^{\alpha_0}p_1^{\alpha_1}\dots p_k^{\alpha_k}$, where p_l are distinct odd primes, the largest natural number t_l such that $(p_l^{t_l}+3)/2 \leq i$ and letting $\Phi_{m,i} = \prod_{p_l|m} p_l^{t_l}$.

We note here that $\Phi_{m,i}$ is obviously multiplicative in that for $(m,n) = 1$, $\Phi_{mn,i} = \Phi_{m,i}\Phi_{n,i}$.

Lemma 3.19 *For all primes p, for $\alpha \in \mathbb{N}$ and $i \geq 2$, $\Phi_{p^{\alpha},i} = \Phi_{p,i}$.*

Proof. Since, by definition, the power of a prime in the prime decomposition of m is not used in computing $\Phi_{m,i}$, the lemma holds. □

Proposition 3.20 *For the group D_{2p}^i, $i \geq 2$, presented as above and p a prime, $\pi_{p,i} = \Phi_{p,i}$.*

Proof. Let p be a fixed odd prime. We use induction on i, so $\pi_{p,k} = \Phi_{p,k}$ for $k < i$.

- $i = 2$.

It follows by Lemma 3.10 that $\pi_{p,2} = 1$ and by definition that $\Phi_{p,2} = 1$.

We now prove the result for i. First we note that $\pi_{p,i}$ forms a monotonic increasing sequence by Lemma 3.8. There are two cases to consider:

1. $\pi_{p,i-1} = \pi_{p,i}$;

2. $\pi_{p,i-1} < \pi_{p,i}$.

• Case 1, $\pi_{p,i-1} = \pi_{p,i}$.

There are two possibilities for the value of $\Phi_{p,i}$; either $\Phi_{p,i-1} = \Phi_{p,i}$ or $\Phi_{p,i-1} < \Phi_{p,i}$. We will assume the latter case and reach a contradiction and so obtain $\Phi_{p,i} = \Phi_{p,i-1} = \pi_{p,i-1} = \pi_{p,i}$, the desired result.

Assume that $\Phi_{p,i} > \Phi_{p,i-1}$. If $\Phi_{p,i-1} = p^c$, where $c = \lfloor \log_p(2(i-1)-3) \rfloor$, then $\Phi_{p,i} = p^{c+1}$, where $c+1 = \lfloor \log_p(2i-3) \rfloor$. We know that $\pi_{p,i-1} = \pi_{p,i}$ so, using Proposition 2.6 and Lemma 3.3, the prime p divides

$$z_{l+(2i-1)} = \frac{2^{2i-3}\bar{l}(\bar{l}+1)\dots(\bar{l}+(2i-1)-3)}{((2i-1)-2)!},$$

where $\bar{l} = LEN(D^i_{2p})/(2i+1) = 2p\pi_{p,i}/(4,p)$. But $p^c = \pi_{p,i-1}$, so $\bar{l} = 2p.p^c = 2p^{c+1}$ giving

$$\begin{aligned} z_{l+(2i-1)} &= \frac{2^{2i-3}(2p^{c+1})(2p^{c+1}+1)\dots(2p^{c+1}+2i-4)}{(2i-3)!} \\ &= 2^{2i-3}\left(\frac{2p^{c+1}}{2i-3}\right)\left(\frac{2p^{c+1}+1}{1}\right)\left(\frac{2p^{c+1}+2}{2}\right)\cdots\left(\frac{2p^{c+1}+2i-4}{2i-4}\right). \end{aligned}$$

Note that the *bth* bracketed term, $2 \le b \le 2i-3$, in the above product may be written as $\left(\frac{2p^{c+1}+p^i m_b}{p^i m_b}\right)$, where $(m_b, p) = 1$ and $0 \le i \le c+1$ (this last inequality follows from the definition of c). Carrying out the obvious simplification we obtain $\left(\frac{2p^{c+1-i}+m_b}{m_b}\right)$. Now notice that $(\prod_{b=2}^{2i-3} m_b)$ is coprime to p. Recall that $p | z_{l+(2i-1)}$ and, by assumption, $\lfloor \log_p(2i-3) \rfloor = c+1$ or $2i-3 = p^{c+1}$. From this last equation it follows that $p \not| z_{l+(2i-1)}$, a contradiction. Hence $\Phi_{p,i} = p^c = \Phi_{p,i-1} = \pi_{p,i-1} = \pi_{p,i}$.

• Case 2, $\pi_{p,i-1} < \pi_{p,i}$.

Let $l = 2p\pi_{p,i-1}$. So by Lemma 3.3 we have $l = 2p^k$ for some integer k. Using Proposition 2.6 for $3 \leq n \leq 2i$ gives

$$\begin{aligned} z_{l+n} &= \frac{2^{n-2}2p^k(2p^k+1)\dots(2p^k+n-3)}{(n-2)!} \\ &= 2^{n-2}\left(\frac{2p^k}{n-2}\right)\left(\frac{2p^k+1}{1}\right)\left(\frac{2p^k+2}{2}\right)\cdots\left(\frac{2p^k+n-3}{n-3}\right). \end{aligned}$$

Since $\pi_{p,i-1} < \pi_{p,i}$ we must have $p \not| z_{l+2i-1}$ or $p \not| z_{l+2i}$. Using an argument similar to that given above we see that $p^k = (2i-1)-2$ or $p^k = (2i)-2$. Hence $k = \lfloor \log_p(2i-3) \rfloor$. Finally by Lemma 3.3 we have $\pi_{p,i} = p^{k-1}.p = p^k$, and so $p^{k-1} = \pi_{p,i-1} = \Phi_{p,i-1}$ and $p^k = \Phi_{p,i} = \pi_{p,i}$. □

Theorem 3.21 *For $i \geq 2$, $LEN(D^i_{2m}) = \Phi_{m,i} MinLEN(D^i_{2m})$.*

Proof. Let $(m,n) = 1$ where $m = p_1^{\alpha_1}\dots p_r^{\alpha_r}$ and $n = q_1^{\beta_1}\dots q_t^{\beta_t}$ with p_i and q_i primes. We have

$$\begin{aligned} \pi_{mn,i} &= \pi_{m,i}\pi_{n,i} \text{ by Lemma 3.9} \\ &= \pi_{p_1^{\alpha_1}\dots p_r^{\alpha_r},i}\pi_{q_1^{\beta_1}\dots q_t^{\beta_t},i} \\ &= \pi_{p_1^{\alpha_1},i}\dots\pi_{p_r^{\alpha_r},i}\pi_{q_1^{\beta_1},i}\dots\pi_{q_t^{\beta_t},i} \text{ by Lemma 3.9} \\ &= \pi_{p_1,i}\dots\pi_{p_r,i}\pi_{q_1,i}\dots\pi_{q_t,i} \text{ by Lemma 3.10} \\ &= \Phi_{p_1,i}\dots\Phi_{p_r,i}\Phi_{q_1,i}\dots\Phi_{q_t,i} \text{ by Proposition 3.20} \\ &= \Phi_{p_1^{\alpha_1},i}\dots\Phi_{p_r^{\alpha_r},i}\Phi_{q_1^{\beta_1},i}\dots\Phi_{q_t^{\beta_t},i} \text{ by Lemma 3.19} \\ &= \Phi_{p_1^{\alpha_1}\dots p_r^{\alpha_r},i}\Phi_{q_1^{\beta_1}\dots q_t^{\beta_t},i} \\ &= \Phi_{m,i}\Phi_{n,i} \\ &= \Phi_{mn,i} \end{aligned}$$

Now since, by definition, $LEN(D^i_{2m}) = \pi_{m,i} MinLEN(D^i_{2m})$ we have $LEN(D^i_{2m}) = \Phi_{m,i} MinLEN(D^i_{2m})$. □

Corollary 3.22

$$LEN(D_{2m}^2) = 10m/(4,m)$$

Proof. In this case, for $m = 2^{\alpha_0}p_1^{\alpha_1}\dots p_k^{\alpha_k}$ where p_l are distinct odd primes, we have $t_l = \lfloor \log_{p_l}(1) \rfloor = 0$ giving $\Phi_{m,2} = 1$. So by Theorem 3.21 we have $LEN(D_{2m}^2) = MinLEN(D_{2m}^2) = 10m/(4,m)$. □

Corollary 3.23

$$LEN(D_{2m}^3) = 14m\Phi_{m,3}/(4,m)$$

where $\Phi_{m,3} = 3$ *if* $m \equiv 0 \bmod 3$, *and* $\Phi_{m,3} = 1$ *otherwise.*

Proof. Using the same notation as in the proof of the previous corollary we obtain $t_l = \lfloor \log_{p_l}(3) \rfloor$ which is equal to 1 if $p_l = 3$ and 0 otherwise. □

We now compare the the efficiency of computer programs to calculate the Fibonacci length of D_{2m}^i for various values of m and i. We use the general **fpfl** program and compare it to a program written for GAP using the main results in this section.

i	m	**fpfl**(D^i_{2m})	time*	$\Phi_{m,i} MinLEN(D^i_{2m})$	time*
2	5	50	130	50	0
2	6	30	140	30	0
2	7	70	140	70	0
2	8	20	160	20	0
3	5	70	260	70	0
3	6	126	470	126	0
3	7	98	660	98	0
3	8	28	870	28	0
4	5	450	2980	450	0
4	6	162	5520	162	0
4	7	126	10110	126	0
4	8	36	16510	36	0

$*$ Time is in milliseconds of cpu time.

4 Other dihedral group generators

We now examine a presentation that is dependent on a parameter m and defines D^2_{2m} when m is odd.

Lemma 4.1 *Let G_m be the group defined by the presentation*

$$\langle\, x,\ y \mid x^{2m} = 1,\ (x^m y)^2 = 1,\ y^{2m} = (xy)^2 \,\rangle$$

where m is an even integer. Then G_m is a covering group of D_{2m}.

Proof. Let m be an even integer. We examine the defining properties of a covering group. Let $A = \langle x^m \rangle$ and let G_m be the group defined by the presentation

$$\langle\, x,\ y \mid x^{2m} = 1,\ (x^m y)^2 = 1,\ y^{2m} = (xy)^2 \,\rangle.$$

- $A \leq G'_m \cap Z(G_m)$

A presentation for G_m/G'_m is given by

$$\begin{aligned} & \langle\, x,\ y \mid x^{2m} = 1,\ (x^m y)^2 = 1,\ y^{2m} = (xy)^2,\ [x,y] = 1 \,\rangle \\ \cong\ & \langle\, x,\ y \mid x^2 = 1,\ y^2 = 1,\ [x,y] = 1 \,\rangle. \end{aligned}$$

Thus $x^m = 1$ holds in the group G_m/G'_m and so $x^m \in G'_m$.

Now we can see that $y^{2m} \in Z(G_m)$ since $G_m = \langle y, xy \rangle$. From $y^{2m} = (xy)^2$ and $(x^m y)^2 = 1$ we get

$$x^{m-1}y^{2m} = x^m yxy = y^{-1}x^{m+1}y.$$

Raising this to the power $2m$ gives

$$x^{2m(m-1)}y^{4m^2} = y^{-1}x^{2m(m+1)}y$$

so $y^{4m^2} = 1$ and $x^{2m} = 1$. Raising $x^{m-1}y^{2m} = y^{-1}x^{m+1}y$ to the power m gives

$$x^{m(m-1)}y^{2m^2} = y^{-1}x^{m(m+1)}y.$$

Since $x^{2m} = 1$ and m is even we get

$$x^m y^{2m^2} = y^{-1}x^m y,$$

or equally

$$yx^m y^{2m^2} = x^m y.$$

We now return to the relation $x^{m-1}y^{2m} = y^{-1}x^{m+1}y$ and see that

$$x^{m-1}y^{2m} = y^{-1}x^{m+1}y = y^{-1}x\underline{x^m y} = y^{-1}xyx^m y^{2m^2}$$

but, again, $y^{2m} \in Z(G_m)$ so

$$x^{m-1}y^{2m}x^m = y^{2m^2}y^{-1}xy.$$

But y^{2m} is central so

$$x^{-1}y^{2m} = y^{2m^2}y^{-1}xy.$$

So postmultiplying by x gives

$$y^{2m} = y^{2m^2}y^{-1}\underline{xyx},$$

but $xyxy = y^{2m}$ so $xyx = y^{2m-1}$ giving

$$\begin{aligned} y^{2m} &= y^{2m^2}y^{-1}y^{2m-1} \\ y^{2m^2-2} &= 1. \end{aligned}$$

Now the order of y is a divisor of $(4m^2, 2m^2-2) = (4m^2, 2(m^2-1)) = 2$. Thus $y^2 = 1$. From $(x^m y)^2 = 1$ we get $x^m y = yx^m$ and so $x^m \in Z(G_m)$.

- $G_m/\langle x^m \rangle \cong D_{2m}$

  A presentation for $G_m/\langle x^m \rangle$ is

$$\begin{aligned} & \langle\, x,\ y \mid x^{2m} = 1,\ (x^m y)^2 = 1,\ y^{2m} = (xy)^2,\ x^m = 1 \,\rangle \\ \cong\ & \langle\, x,\ y \mid x^m = 1,\ y^2 = 1,\ (xy)^2 = 1 \,\rangle \end{aligned}$$

The last presentation above is the standard presentation for D_{2m}.

- $|A| = |M(D_{2m})|$

  From the presentation for G_m we see that x^m has order two and so $|A| = 2$ and it is well known that $M(D_{2m}) = C_2$ for even m and so $|M(D_{2m})| = 2$.

  Thus G_m is a covering group of D_{2m} when m is even. □

Lemma 4.2 *The presentation*

$$\langle\, x,\ y \mid x^{2m} = 1,\ (x^m y)^2 = 1,\ y^{2m} = (xy)^2 \,\rangle$$

with m even defines a group isomorphic to $D_{2(2m)}$.

Proof. Let m be an even integer. First recall that in the proof of the previous lemma it was shown that the element x^m is central in the group defined by the presentation $\langle\ x,\ y \mid x^{2m} = 1,\ (x^m y)^2 = 1,\ y^{2m} = (xy)^2\ \rangle$. So $(x^m y)^2 = 1$ becomes $y^2 = x^{-2m} = 1$ giving $(xy)^2 = y^{2m} = 1$ and the group defined by the presentation is isomorphic to $D_{2(2m)}$ which can be presented by $\langle\ x,\ y \mid x^{2m} = y^2 = (xy)^2 = 1\ \rangle$.

Alternatively note that this result follows immediately from the result $x^m \in Z(G_m)$ and Lemma 4.1. □

Theorem 4.3 *For m odd, D_{2m}^2 is defined by the presentation*

$$\langle\ x,\ y \mid x^{2m} = 1,\ (x^m y)^2 = 1,\ y^{2m} = (xy)^2\ \rangle.$$

Proof. See [22] for more information. □

Theorem 4.4 *For a given integer m, let G_m be the group defined by the presentation*

$$\langle\ x,\ y \mid x^{2m} = 1,\ (x^m y)^2 = 1,\ y^{2m} = (xy)^2\ \rangle.$$

Then G_m has Fibonacci length 6.

Proof. There are two cases to consider, namely m even and m odd.

- m even.

When m is even we have seen that the presentation is in fact equivalent to

$$\langle\ x,\ y \mid x^{2m} = 1,\ y^2 = 1,\ (xy)^2 = 1\ \rangle$$

which defines the dihedral group $D_{2(2m)}$ and so by [19] has Fibonacci length 6.

- m odd.

That the presentation defines D_{2m}^2 is shown in [22]. We first show that the following relations hold in the presentation for D_{2m}^2, m odd:

$$xy^2xy^2xyxy^2xy = x$$

and

$$yxyxy^2xyxy^2xy^2xyxy^2xy = y.$$

In [22] it is shown that the following also hold in the presentation for D_{2m}^2:

$$\begin{array}{llll} \text{(i)} & y^{2m} = 1, & \text{(ii)} & (xy)^2 = 1, \\ \text{(iii)} & xy^{m-1}x^{-1} = y^{-m+1}, & \text{(iv)} & y^{-m}xy^m = x^{-1}. \end{array}$$

Now

$$1 = xy^{m-1}x^{-1}xy^{m+1}x^{-1} \text{ by (i)}$$

and

$$1 = \underline{xy^{m-1}x^{-1}}xy^{m+1}x^{-1} = y^{-m+1}xy^{m+1}x^{-1} \text{ by (iii)}.$$

We now have

$$1 = y\underline{y^{-m}xy^m}yx^{-1} = yx^{-1}yx^{-1} \text{ by (iv)}.$$

Now using (ii) we see that

$$1 = yx^{-1}y\underline{x^{-1}} = yx^{-1}y^2xy = y\underline{x^{-1}}yxyxy^2xy = y^2xy^2xyxy^2xy.$$

Thus $xy^2xy^2xyxy^2xy = x$ in D_{2m}^2 , m odd.

The second result follows since

$$yxyxy^2xy\underline{xy^2xy^2xyxy^2xy} = y\underline{xyxy}yyxyx = y\underline{yyxyx} = y.$$

So G_m, m odd, is a homomorphic image of $F(2,6)$. To see this we write down the standard presentation for $F(2,6)$

$$\langle\, a,b,c,d,e,f \quad | \quad ab=c, bc=d, cd=e, de=f, ef=a, fa=b \,\rangle$$

Now rewriting the relations we have

$$\begin{aligned} d &= bc = bab \\ e &= cd = ab^2ab \\ f &= de = babab^2ab \\ a &= ef = ab^2ab^2abab^2ab \\ b &= fa = babab^2abab^2ab^2abab^2ab. \end{aligned}$$

In fact we have shown that $F(2,6)$ can be defined by the presentation

$$\langle\, x,y \quad | \quad x = xy^2xy^2xyxy^2xy, y = yxyxy^2xyxy^2xy^2xyxy^2xy \,\rangle.$$

So G_m, m odd, is a homomorphic image of $F(2,6)$. Using the fact that $6 = \min\{n : |F(2,n)| \text{ is infinite}\}$ it follows that $LEN(G_m) = 6$ for odd m. □

Remark 4.5 Relating this result to that of Corollary 3.22 we see that the generating set for D_{2m}^2, m odd, used in this section always gives a constant Fibonacci length of 6 while the generating set used in the previous section for D_{2m}^2 gives a Fibonacci length of $10m/(4,m) = 10m$, which is always greater than 6.

Remark 4.6 It is interesting to note that all Fibonacci lengths in this chapter have been even numbers and so are Wall numbers.

Open question The above raises the following natural question: For every D_{2m}^i does there exist a generating set X such that $LEN_X(D_{2m}^i) = 6$ i.e. is every D_{2m}^i an epimorphic image of $F(|X|,6)$? A related question is to prove, or disprove,

the existence of epimorphisms φ and ψ in the following diagram (all maps that are not named are epimorphisms):

$$\begin{array}{ccc} F(|X|,6) & \longrightarrow & D_{2m} \\ \psi \uparrow & \searrow \varphi & \uparrow \\ F(|X|,w) & \longrightarrow & D_{2m}^{i} \end{array}$$

where $i \geq 2$.

Chapter 5

The efficiency of direct powers of the group defined by $\langle\, a,\ b \mid a^2,\ b^p,\ (ab^2)^4,\ (abab^2)^3 \,\rangle$

1 Introduction

In this chapter we will prove that the group $G(p)$ with the presentation

$$\langle\, a,\ b \mid a^2,\ b^p,\ (ab^2)^4,\ (abab^2)^3 \,\rangle$$

where p is an odd prime, is efficient and furthermore we will show that the groups $G(p)^n$, the direct product of n copies of $G(p)$, are also efficient. To do this we will use results from [23] to show that one only needs to find efficient presentations for $G(p)^m$, $m \in \{1, 2, 3\}$ and from this one may use an induction argument from [23] to show that $G(p)^n$, $n \in \mathbb{N}$, is efficient.

The above presentation was first studied in [55] and later in [40]. It was proved in [40] that $G(p)$, p an odd prime, is isomorphic to $PGL(2, p)$ if the congruence $x^2 \equiv 2 \bmod p$ has no solutions in the integers and is $PSL(2, p) \times C_2$ otherwise.

For further details of $PGL(2,p)$ and $PSL(2,p)$ see Chapter 6, Section 2.

Some of the results in this chapter are to appear in the paper "On the efficiency of direct powers of $PGL(2,p)$", see [18].

2 Preliminaries

Definition 2.1 Let p be an odd prime. We denote by $G(p)$ the group defined by the presentation

$$\langle\, a,\ b \mid a^2,\ b^p,\ (ab^2)^4,\ (abab^2)^3 \,\rangle.$$

In order for us to prove that direct product of copies of the group $G(p)$ are efficient on a minimal generating set we need to find some properties of its minimal generating sets and its Schur multiplier. We first need some definitions.

Definition 2.2 Given a finitely generated group G we denote by $d(G)$ the minimum number of generators needed to generate G. If G^n denotes the group constructed by taking the direct product of n copies of G then the *growth sequence* of the finite group G is the sequence $(d(G^n))_{n=1}^{\infty}$.

The following results regarding $d(G^n)$ were proved in [72]:

Theorem 2.3 *Let G be a finite imperfect group with the rank of G/G' being k. Then there is a least integer n_0 such that $d(G^n) = nk$, for all $n \geq n_0$. Furthermore*

(i) *if all simple images of G are abelian then $n_0 \leq d(G)/k$,*

(ii) *if the order of the smallest nonabelian simple image of G is denoted by s and if n_1 is the smallest positive integer solution of*

$$kn \geq d(G) + 1 + \log_s n$$

we have $n_0 \leq n_1$.

Definition 2.4 The quantity n_0 in the theorem above is called the *growth index* of G.

There are several results that let us calculate the growth index of a group G. One such result is given in [23] and we reproduce it here together with its proof:

Lemma 2.5 *If G is a finite imperfect group with non abelian simple images and is generated by two elements of coprime order then the growth index of G is two.*

Proof. Suppose $G = \langle x, y \rangle$ where the order of x is q, the order of y is r and $(q, r) = 1$.

Consider the elements $u = (x, y)$ and $v = (y, x)$ of $G \times G$. Since $(q, r) = 1$, there exist integers λ and μ such that $\lambda q + \mu r = 1$. Then $u^{\lambda q} = (1, y)$, $u^{\mu r} = (x, 1)$, $v^{\lambda q} = (y, 1)$ and $v^{\mu r} = (1, x)$. Thus $G \times G$ is two generated. Similarly it may be shown that $G \times G \times G = G^3$ may be generated by the three elements $u = (x, x, y)$, $v = (y, x, y)$ and $w = (y, y, x)$, and therefore, G has growth index two. □

As an immediate consequence of this we have

Corollary 2.6 *The group $G(p)$, where p is an odd prime, has growth index two.*

We now need some definitions and results concerning the Schur multiplier of $G(p)$, written $M(G(p))$. We start with:

Lemma 2.7 *For p an odd prime we have, $M(G(p)) \cong C_2$.*

Proof. If $G(p) \cong PGL(2, p)$ then it is well known that $M(PGL(2, p)) \cong C_2$, see [43]. If, on the other hand, $G(p) \cong C_2 \times PSL(2, p)$ then we use the Schur-Künneth

formula:

$$\begin{aligned} M(C_2 \times PSL(2,p)) &\cong M(C_2) \times M(PSL(2,p)) \times (C_2 \otimes PSL(2,p)), \\ &\cong \{id\} \times C_2 \times (C_2/C_2' \otimes PSL(2,p)/PSL(2,p)'), \\ &\cong C_2. \end{aligned}$$

We note here that when $p = 3$ the congruence $x^2 \equiv 2 \bmod p$ has no integer solutions so $G(3) \cong PGL(2,3)$. Thus $M(G(p)) \cong C_2$ as required. □

In [55] the following presentation for $G(p)$ was obtained:

$$\langle\, a, b \mid a^2 b^p, (ab^2)^4, (abab^2)^3 b^p \,\rangle \tag{5.1}$$

From this and the last result concerning the Schur multiplier of $G(p)$ we have:

Theorem 2.8 *The group $G(p)$, p an odd prime, is efficient.*

Proof. This follows from noting that $\text{rank}(C_2) = 1$ and the deficiency of (5.1) is one. □

From the Schur-Künneth formula and the fact that $G^n \otimes G = (G \otimes G)^n$ it can be shown by induction that $M(G^n) = M(G)^n \times (G \otimes G)^{\binom{n}{2}}$. It follows that the rank of $M(G^n)$ is at most $nm + \binom{n}{2} k^2$ where $k = \text{rank}(G/G')$ and $m = \text{rank}(M(G))$.

Definition 2.9 Let G be a finite group. We denote the sequence $(\text{rank}(M(G^n)))_{n=1}^{\infty}$ by $(m_G(n))_{n=1}^{\infty}$. The *multiplier index* of G is the least integer, n, such that $m_G(n) = n(m-j) + \binom{n}{2} k^2$, where $k = \text{rank}(G/G')$, $m = \text{rank}(M(G))$ and j is the number of the cyclic factors of $M(G)$ whose orders are coprime to at least one of the orders of the cyclic factors of G/G'.

Remark 2.10 We know that in the above definition such an n will exist. For if j is positive then the coprime factors in the abelian decomposition of $M(G^n)$ will not contribute to the rank for large enough n and the rank will tend to $n(m-j)+\begin{pmatrix} n \\ 2 \end{pmatrix}k^2$.

We will need to calculate $G(p)/G(p)'$ to find the multiplier index of $G(p)$.

Lemma 2.11 *For p an odd prime, $G(p)/G(p)' \cong C_2$.*

Proof. We use the matrix method to prove the assertion. Let p be an odd prime. The relation matrix of $\langle\ a,\ b \mid a^2=1,\ b^p=1,\ (ab^2)^4=1,\ (abab^2)^3=1\ \rangle$ is

$$\begin{pmatrix} 2 & 0 \\ 0 & p \\ 4 & 8 \\ 6 & 9 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 0 \\ 0 & p \\ 0 & 8 \\ 0 & 9 \end{pmatrix}$$

$$\longrightarrow \begin{pmatrix} 2 & 0 \\ 0 & p \\ 0 & 8 \\ 0 & 1 \end{pmatrix}$$

$$\longrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 2 \\ 0 & 0 \\ 0 & 0 \end{pmatrix},$$

so $G(p)/G(p)' \cong C_2$ as required.

Alternatively this result follows from noting that $G(p) \cong PGL(2,p)$ or $PSL(2,p) \times C_2$. □

So $G(p)$ is an imperfect group with $G(p)/G(p)'$ isomorphic to C_2. Thus

Lemma 2.12 *The multiplier index of $G(p)$, p an odd prime, is two.*

Proof. We have $k = \text{rank}(G/G') = \text{rank}(C_2) = 1$, $m = \text{rank}(M(G)) = \text{rank}(C_2) = 1$ and $j = 0$, where j is the number of the cyclic factors of $M(G)$ whose orders are coprime to at least one of the orders of the cyclic factors of G/G'. So from Definition 2.9 we need to find the smallest solution n of

$$\begin{aligned} m_G(n) &= n(m-j) + \binom{n}{2} k^2 \\ &= n + \binom{n}{2}. \end{aligned}$$

By performing the calculations, see Lemma 3.1, for $m_{G(p)}(2) = 3$, we see that the smallest integer satisfying this equation is $n = 2$. Thus the multiplier index of $G(p)$ is two. □

We are almost at the stage where we are able to state how many efficient presentations we need to find to show that $G(p)^n$ is efficient on a minimal generating set, where p is an odd prime and n is any natural number. We need the following definition:

Definition 2.13 Let G be a finite imperfect group and let r_0 be the maximum of the growth index and the multiplier index, then G is said to attain *quadratic efficiency* at i if $i \geq r_0$ and G^i has a minimal efficient presentation.

We now state the result from [23] that gives us a condition that lets us prove $G(p)^n$ is efficient on a minimal generating set.

Theorem 2.14 *Let G be an imperfect finite group with G/G' of rank one and growth index two. Then if $M(G)$ is trivial or is cyclic with $(|M(G)|, |G/G'|) \neq 1$ and G attains quadratic efficiency at 2 and 3, then G attains quadratic efficiency at n for all $n \geq 2$.*

Proof. See [23] for the proof. □

As a consequence of this theorem we have:

Corollary 2.15 *Let p be an odd prime. If $G(p)^n$ attains quadratic efficiency at $n = 2$ and 3 then $G(p)^n$, $n \geq 2$, is efficient on a minimal generating set.*

The rest of this chapter will be dedicated to finding efficient presentations for $G(p)^2$ and $G(p)^3$.

3 The efficiency of $G(p)^2$, p an odd prime

If we are going to find an efficient presentation for $G(p)^2$, p an odd prime, we will need to calculate the Schur multiplier of $G(p)^2$, so we have:

Lemma 3.1 $M(G(p)^2) \cong C_2^3$.

Proof. We use the Schur-Künneth formula as follows:

$$\begin{aligned} M(G(p)^2) &\cong M(G(p)) \times M(G(p)) \times (G(p) \otimes G(p)), \\ &\cong M(G(p)) \times M(G(p)) \times (G(p)/G(p)' \otimes G(p)/G(p)'), \\ &\cong C_2 \times C_2 \times (C_2 \otimes C_2), \\ &\cong C_2^3. \end{aligned}$$

Hence the result holds. □

We first find a presentation for $G(p)^2$ on two generators using the following easily proved lemma, see [45].

Lemma 3.2 *If G, H are groups presented by $\langle X \mid R \rangle$, $\langle Y \mid S \rangle$ respectively, then their direct product $G \times H$ has the presentation $\langle X, Y \mid R, S, [X,Y] \rangle$, where $[X,Y]$ denotes the set of commutators $\{ x^{-1}y^{-1}xy \mid x \in X, y \in Y \}$.* □

Using the previous lemma we are now able to give a presentation for $G(p)^2$ on two generators.

Lemma 3.3 *A presentation for $G(p)^2$ is*

$$\begin{aligned} \langle x, y \mid\ & x^{2p} = y^{2p} = x^{-4}(xy^2)^4 = y^{-4}(yx^2)^4 = 1, \\ & y^{-p}(x^pyx^py^2)^3 = x^{-p}(y^pxy^px^2)^3 = [x^p, y^p] = [x^2, y^2] = 1 \rangle. \end{aligned} \tag{5.2}$$

Proof. Since $G(p)$ is the group defined by the presentation

$$\langle a, b \mid\ a^2 = b^p = (ab^2)^4 = (abab^2)^3 = 1 \rangle$$

the standard presentation for the group $G(p) \times G(p)$ is

$$\begin{aligned} \langle a, b, c, d \mid\ & a^2 = b^p = (ab^2)^4 = (abab^2)^3 = 1, \\ & c^2 = d^p = (cd^2)^4 = (cdcd^2)^3 = 1, \\ & [a,c] = [a,d] = [b,c] = [b,d] = 1 \rangle. \end{aligned}$$

Now let $x = ad$ and $y = bc$. So $x^p = a$ giving $d = x^{1-p}$, likewise we get $y^p = c$ and $b = y^{1-p}$. Now let us rewrite the relations in terms of x and y.

$$\begin{aligned}
a^2 = 1 &\longrightarrow x^{2p} = 1, \\
b^p = 1 &\longrightarrow y^{p(1-p)} = 1, \\
(ab^2)^4 = 1 &\longrightarrow (x^p y^{2(1-p)})^4 = 1, \\
(abab^2)^3 = 1 &\longrightarrow (x^p y^{(1-p)} x^p y^{2(1-p)})^3 = 1, \\
c^2 = 1 &\longrightarrow y^{2p} = 1, \\
d^p = 1 &\longrightarrow x^{p(1-p)} = 1, \\
(cd^2)^4 = 1 &\longrightarrow (y^p x^{2(1-p)})^4 = 1, \\
(cdcd^2)^3 = 1 &\longrightarrow (y^p x^{(1-p)} y^p x^{2(1-p)})^3 = 1, \\
[a, c] = 1 &\longrightarrow [x^p, y^p] = 1, \\
[a, d] = 1 &\longrightarrow [x^p, x^{1-p}] = 1, \\
[b, c] = 1 &\longrightarrow [y^{1-p}, y^p] = 1, \\
[b, d] = 1 &\longrightarrow [y^{1-p}, x^{1-p}] = 1.
\end{aligned}$$

Since p is an odd prime the relation $x^{2p} = 1$ implies $x^{p(1-p)} = 1$ and this relation is redundant. Similarly $y^{p(1-p)} = 1$ is redundant.

Obviously removing the relators $[x^p, x^{1-p}] = 1$ and $[y^{1-p}, y^p] = 1$ does not affect the group that the presentation defines.

Now we examine the relations $[x^p, y^p] = 1$ and $[y^{1-p}, x^{1-p}] = 1$. Since $y^{2p} = 1$ we have $1 = [y^{1-p}, x^{1-p}] = [y^{1+p}, x^{1-p}]$ and so $1 = [y^{1-p}y^{1+p}, x^{1-p}] = [y^2, x^{1-p}]$ and using the same argument on the right hand side of the square brackets we see that $1 = [y^2, x^2]$. Obviously the last relation implies $[y^{1-p}, x^{1-p}] = 1$.

Finally we 'tidy up' the remaining relations. Since $1 = y^{2p}$ we have $1 = (x^p y^{2(1-p)})^4 = (x^p y^2)^4$, and using $1 = [y^2, x^2]$ we obtain

$$\begin{aligned} 1 &= (x\underline{x^{p-1}}y^2)^4, \\ &= \underline{x^{4(p-1)}}(xy^2)^4, \\ &= x^{-4}(xy^2)^4. \end{aligned}$$

Using an analogous argument we may show that $y^{-4}(yx^2)^4 = 1$. From $(x^p y^{(1-p)} x^p y^{2(1-p)})^3 = 1$ together with $[y^2, x^2] = 1$ and $y^{2p} = 1$ we get

$$\begin{aligned} 1 &= (x^p y^{(1-p)} x^p \underline{y^{2(1-p)}})^3, \\ &= (x^p \underline{y^{(1-p)}} x^p y^2)^3, \\ &= \underline{y^{-3p}}(x^p y x^p y^2)^3, \\ &= y^{-p}(x^p y x^p y^2)^3. \end{aligned}$$

Again we can also use a similar argument to show that $x^{-p}(y^p x y^p x^2)^3 = 1$. □

We can now start to remove redundant relations from (5.2).

Lemma 3.4 *The relation $x^{2p} = 1$ is redundant in presentation* (5.2).

Proof. Since $(2, p) = 1$, by the Euclidean algorithm there exist integers λ and μ such that $1 = 2\lambda + p\mu$. So using the last two relations of (5.2) we have that

$$\begin{aligned} x^{2p}y &= x^{2p}y^{2\lambda+p\mu}, \\ &= y^{2\lambda}x^{2p}y^{p\mu}, \text{ since } [x^2, y^2] = 1, \\ &= y^{2\lambda+p\mu}x^{2p}, \text{ since } [x^p, y^p] = 1, \\ &= yx^{2p}, \end{aligned}$$

and so $x^{2p} \in Z(G(p)^2)$. It is also easily seen that $x^2 = 1$ in $G(p)^2/G(p)^{2\prime}$. Thus x^{2p} is contained within the Schur multiplier, C_2^3, of $G(p)^2$, giving $x^{4p} = 1$.

The third relation of (5.2), namely $x^{-4}(xy^2)^4 = 1$, together with $x^{4p} = 1$ gives $x^{4(p-1)}(xy^2)^4 = 1$, but since $[x^2, y^2] = 1$ we have

$$\begin{aligned} 1 &= \underline{x^{4(p-1)}}xy^2xy^2xy^2xy^2, \\ &= x^{3(p-1)}xy^2xy^2xy^2\underline{x^{p-1}xy^2}, \\ &= x^{3(p-1)}xy^2xy^2xy^2x^py^2. \end{aligned}$$

Continuing in this way we finally obtain $(x^py^2)^4 = 1$. This relation gives $yx^py^2x^py = (yx^py^2x^py)^{-1}$. Substituting the last relation into the relation $y^{-p}(x^pyx^py^2)^3 = 1$ gives

$$\begin{aligned} y^p &= \underline{x^py}x^py^2x^pyx^py^2x^pyx^py^2, \\ y^p &= yx^py^2x^pyx^py^2x^pyx^py^2x^p, \text{ since } [x^p, y^p] = 1, \\ y^{p+1} &= \underline{yx^py^2x^py}x^py^2x^pyx^py^2x^py, \\ y^{p+1} &= (yx^py^2x^py)^{-1}x^py^2x^p(yx^py^2x^py) \end{aligned}$$

and, on raising this to the power p while using the facts that $[x^2, y^2] = 1$ and $y^{2p} = 1$, we get $1 = y^{p(p+1)} = x^{2p^2}$. Since $(2p^2, 4p) = 2p$ we have $x^{2p} = 1$. □

Note that in the above proof examples that the values λ and μ could take are $\lambda = (p+1)/2$ and $\mu = -1$ or any multiple of these values.

Lemma 3.5 *The two relations* $y^{2p} = 1$ *and* $y^{-4}(yx^2)^4 = 1$ *imply* $[x^2, y^2] = 1$.

Proof. From $y^4 = (yx^2)^4$ we have $[y^4, yx^2] = 1$, or $[y^4, x^2] = 1$. Since $(2, p) = 1$ there exist integers λ and μ satisfying $2\lambda + p\mu = 1$. Thus $y^2 = y^{4\lambda+2p\mu} = y^{4\lambda}$ since $y^{2p} = 1$. Now $[y^4, x^2] = 1 \Rightarrow [y^{4\lambda}, x^2] = 1 \Rightarrow [y^2, x^2] = 1$. So x^2 and y^2 commute. (If $\lambda < 0$ then $1 = [y^4, x^2]$ gives $1 = y^{-4}x^{-2}y^4x^2 = x^{-2}y^4x^2y^{-4} = [x^2, y^{-4}] = [y^{-4}, x^2]$ and the result can be proved from here.) □

Now our presentation for $G(p)^2$ is

$$\langle\, x, y \mid y^{2p}, x^{-4}(xy^2)^4, y^{-4}(yx^2)^4, y^{-p}(x^pyx^py^2)^3, x^{-p}(y^pxy^px^2)^3, [x^p, y^p] \,\rangle. \quad (5.3)$$

The deficiency of this presentation is four, which is one more than is allowed to show it efficient. Now we examine the presentation

$$\mathcal{P} = \langle\, x, y \mid x^{-4}(xy^2)^4, y^{-4}(yx^2)^4 y^{2p}, y^{-p}(x^p y x^p y^2)^3, x^{-p}(y^p x y^p x^2)^3, x^{-p}y^{-p}x^p y^{3p} \,\rangle.$$

First we need the following result so that we may use the standard multiplier argument, see for example [20].

Lemma 3.6 *The factor group $\langle\mathcal{P}\rangle/\langle\mathcal{P}\rangle'$ is isomorphic to C_2^2.*

Proof. The relation matrix of $\mathcal{P}$ is

$$\begin{pmatrix} 0 & 8 \\ 8 & 2p \\ 6p & 9-p \\ 9-p & 6p \\ 0 & 2p \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & 8 \\ 8 & 0 \\ 6p & 9-p \\ 9-p & 0 \\ 0 & 2p \end{pmatrix}$$

$$\longrightarrow \begin{pmatrix} 0 & 2 \\ 2 & 0 \\ 6p & 9-p \\ 9-p & 0 \\ 0 & 0 \end{pmatrix}$$

$$\longrightarrow \begin{pmatrix} 2 & 0 \\ 0 & 2 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

So $\langle\mathcal{P}\rangle/\langle\mathcal{P}\rangle' \cong C_2^2$. □

We now show that $y^{2p} = 1$ follows from the relations of $\mathcal{P}$, so that all the relations of (5.3) hold in $\mathcal{P}$.

Lemma 3.7 *In $\langle \mathcal{P} \rangle$ the element x^{2p} is central, and $x^{4p} = 1$.*

Proof. From the third relation of $\mathcal{P}$, $y^{-p}(x^p y x^p y^2)^3 = 1$, we have $[y^p, x^p y x^p] = 1$, and conjugating this by x^p we deduce $[x^{-p}y^p x^p, y x^{2p}] = 1$. The fifth relation, $x^{-p}y^{-p}x^p y^{3p} = 1$, gives us $[y, x^{-p}y^p x^p] = 1$, so $[x^{-p}y^p x^p, x^{2p}] = 1$ i.e. $[y^p, x^{2p}] = 1$.

Now if we examine the relation $y^{-4}(yx^2)^4 y^{2p} = 1$ we get $[x^2, y^{2p-4}] = 1$ giving $[x^{2p}, y^{2p-4}] = 1$ so $[x^{2p}, y^4] = 1$. Since $[x^{2p}, y^p] = 1$, $[x^{2p}, y^4] = 1$, and $p = 4k \pm 1$ ($k \in \mathbb{Z}$) we have $[x^{2p}, y] = 1$, i.e. x^{2p} is central in $\mathcal{P}$. Now applying the standard multiplier argument we have $x^{4p} = 1$. □

Lemma 3.8 *In $\langle \mathcal{P} \rangle$ the elements x^2 and y^2 commute.*

Proof. From Lemma 3.7 we have $[x^{2p}, y] = 1$, and on writing $p = 4\lambda \pm 1$, for $\lambda \in \mathbb{Z}$, we obtain $[x^{8\lambda \pm 2}, y] = 1$. Now the first relation of $\mathcal{P}$ tells us that $[y^2, x^4] = 1$, and so we have $[x^2, y^2] = 1$. □

Lemma 3.9 *In $\mathcal{P}$, $[y^{2p}, x^i y^j x^k] = 1$, where i and k are any odd integers and $j \in \mathbb{Z}$.*

Proof. The relation $x^{-p}y^{-p}x^p y^{3p} = 1$ implies the relations $[y, x^{-p}y^p x^p] = 1$ and $[y, x^{-p}y^{2p}x^p] = 1$. Now using Lemma 3.8 we have $x^{-p}y^{2p}\underline{x^p} = x^{-p}x^{(p-1)}y^{2p}x = x^{-1}y^{2p}x$ and so $[y, x^{-1}y^{2p}x] = 1$ and hence by conjugating by x we obtain $[y^{2p}, xyx^{-1}] = 1$. The last relation gives $[y^{2p}, xy^j x^{-1}] = 1$, $j \in \mathbb{Z}$, and again using Lemma 3.8 we obtain the desired result. (This last statement can be seen when we write out the commutators in full i.e. let $j \in \mathbb{Z}$, $i = 1 + e$ and $k = t - 1$

where e and t are even integers, then:

$$\begin{aligned}
1 &= [y^{2p}, xy^jx^{-1}], \\
&= y^{-2p}xy^{-j}x^{-1}y^{2p}xy^jx^{-1}, \\
&= x^{-t}y^{-2p}xy^{-j}x^{-1}y^{2p}x^{-e+1+e}y^jx^{-1}x^t, \\
&= y^{-2p}x^{1-t}y^{-j}x^{-1-e}y^{2p}x^{1+e}y^jx^{t-1}, \text{ since } [x^2, y^2] = 1, \\
&= y^{-2p}x^{-k}y^{-j}x^{-i}y^{2p}x^iy^jx^k, \\
&= [y^{2p}, x^iy^jx^k].)
\end{aligned}$$

□

Lemma 3.10 *In $\langle \mathcal{P} \rangle$ the element y^{4p} is central, and so $y^{8p} = 1$.*

Proof. From the relation $x^{-p}(y^pxy^px^2)^3 = 1$ in the presentation $\mathcal{P}$ we have $[y^pxy^p, x^p] = 1$, and on conjugating this by y^p we obtain $[y^{-p}x^py^p, xy^{2p}] = 1$ or $[y^{-p}x^py^p, y^{-2p}x^{-1}] = 1$ so $y^{-p}x^py^{-p}x^{-1} = y^{-2p}x^{-1}y^{-p}x^py^p$. Postmultiply the last relation by y^{2p} to obtain $y^{-p}x^py^{-p}x^{-1}y^{2p} = y^{-2p}x^{-1}y^{-p}x^py^{3p}$. By the fifth relation of $\mathcal{P}$, namely $x^{-p}y^{-p}x^py^{3p} = 1$, we may easily deduce that $[x^{-1}, y^{-p}x^py^{3p}] = 1$, and using this we have $y^{-p}x^py^{-p}x^{-1}y^{2p} = y^{-3p}x^py^{3p}x^{-1}$. Using Lemma 3.9 this last relation becomes

$$\begin{aligned}
\underline{y^{-p}x^py^{-p}x^{-1}y^{2p}} &= y^{-3p}x^py^{3p}x^{-1}, \\
y^px^py^{-p}x^{-1} &= \underline{y^{-3p}}x^py^{3p}x^{-1}, \\
y^{4p}x^py^{-p}x^{-1} &= x^py^{3p}x^{-1}
\end{aligned}$$

i.e. $[y^{4p}, x^p] = 1$. So, using this result together with $[y^2, x^2] = 1$ and the Euclidean algorithm, we see that y^{4p} is central, and using the multiplier argument, we have $y^{8p} = 1$ in $\langle \mathcal{P} \rangle$. □

Lemma 3.11 *The relation $xy^{2p} = y^{-2p}x$ holds in $\langle \mathcal{P} \rangle$.*

Proof. From the fifth relation of $\mathcal{P}$, $x^{-p}y^{-p}x^py^{3p} = 1$, and the fact from Lemma 3.7 that x^{2p} is central in $\mathcal{P}$ we may deduce that $x^py^{-p}x^{-p}y^{3p} = 1$ and so a cyclic permutation of this relation gives $x^{-p}y^{3p}x^py^{-p} = 1$. We now form the product $(y^{3p}x^{-p}y^{-p}x^p)(x^{-p}y^{3p}x^py^{-p})$ to get $x^{-p}y^{2p}x^py^{2p} = 1$, and the result follows from this and Lemma 3.8. □

Theorem 3.12 *$\mathcal{P}$ is an efficient presentation for $G(p)^2$ on a minimal generating set.*

Proof. By Lemmas 3.7 and 3.8 the first relation of $\mathcal{P}$ may be written as $(x^py^2)^4 = 1$ as follows:

$$\begin{aligned} 1 &= x^{-4}(xy^2)^4, \\ &= x^{4p}x^{-4}(xy^2)^4, \\ &= x^{3(p-1)}x^{p-1}(xy^2xy^2xy^2xy^2), \\ &= x^{3(p-1)}(xy^2xy^2xy^2x^py^2), \\ &\cdots \quad \cdots, \\ &= (x^py^2)^4. \end{aligned}$$

This last relation can be rewritten as $(yx^py^2x^py)^{-1} = yx^py^2x^py$. Substituting this into the relation $y^{-p}(x^pyx^py^2)^3 = 1$ we obtain $y^p = x^p(yx^py^2x^py)^{-1}x^py^2x^pyx^py^2$. Postmultiplying by x^py gives $y^px^py = x^p(yx^py^2x^py)^{-1}x^py^2x^pyx^py^2x^py$ and noting that $x^p = x^{-3p}$ with x^{-2p} central in $\mathcal{P}$ gives

$$\begin{aligned} y^px^py &= \underline{x^p}(yx^py^2x^py)^{-1}\underline{x^p}y^2x^pyx^py^2x^py, \\ x^{-p}y^px^py &= (yx^py^2x^py)^{-1}\underline{x^{-3p}}y^2x^pyx^py^2x^py, \\ x^{-p}y^px^py &= (yx^py^2x^py)^{-1}x^{-p}y^2x^p(yx^py^2x^py)x^{2p}. \end{aligned}$$

If we now use Lemma 3.11 then, after raising the last relation to the power p, we have $(x^{-p}y^px^py)^p = y^{-2p}x^{2p^2}$ which, on using the fifth relation of $\mathcal{P}$, becomes

$(\underline{x^{-p}y^px^py})^p = (y^{3p+1})^p = y^{-2p}x^{2p^2}$ or

$$y^{3p(p+1)} = x^{2p^2}. \tag{5.4}$$

We now examine separately the cases $p = 8\lambda+1$, $p = 8\lambda-1$, $p = 8\lambda+3$ and $p = 8\lambda+5$ ($\lambda \in \mathbb{Z}$).

Case I $p = 8\lambda+1$

Here (5.4) becomes $y^{3p(8\lambda+2)} = x^{2p(8\lambda+1)}$ which by Lemmas 3.7 and 3.10 gives $y^{6p} = x^{2p}$. If we now cube this relation, and note the orders of the generators, we observe that $y^{8p} = 1$ and so $x^{2p} = y^{2p}$. From the last relation and Lemma 3.8 the second relation of $\mathcal{P}$, $y^{-4}(yx^2)^4y^{2p} = 1$, becomes $(y^px^2)^4y^{2p} = 1$ or $xy^px^2y^px = x^{-1}y^{-p}y^{-2p}x^{-2}y^{-p}x^{-1}$. If we now examine $x^{-p}(y^pxy^px^2)^3 = 1$, the fourth relation of $\mathcal{P}$, and if we use the last relation, the fact that $y^{4p} = 1$, y^{2p} is central in $\mathcal{P}$ and Lemma 3.11, we get

$$\begin{aligned}
1 &= x^{-p}y^pxy^px^2y^pxy^px^2y^pxy^px^2,\\
y^{-p}x^p &= xy^px^2y^pxy^px^2y^pxy^px^2,\\
y^{-p}x^p &= \underline{xy^px^2y^px}y^px^2y^pxy^px^2,
\end{aligned}$$

$$\begin{aligned}
y^{-p}x^p &= (x^{-1}y^px^{-2}y^{-p}x^{-1}y^p)x^2\underline{y^px}y^px^2,\\
y^{-p}x^p &= (x^{-1}y^px^{-2}y^{-p}x^{-1}y^p)x^2y^{-p}xy^px^2y^{2p},\\
y^{-p}x^py^{-p}x &= (x^{-1}y^px^{-2}y^{-p}x^{-1}y^p)x^2y^{-p}xy^px^2y^{-p}xy^{2p},\\
y^{-p}x^py^{-p}x &= (x^{-1}y^px^{-2}y^{-p}x^{-1}y^p)x^2(y^{-p}xy^px^2y^{-p}x)y^{2p}.
\end{aligned}$$

Raise this to the power p to give $(y^{-p}x^py^{-p}x)^p = x^{2p}y^{2p^2}$ and use the last relation of $\mathcal{P}$, Lemmas 3.7 and 3.8, $y^{4p} = 1$ and $y^{2p} = x^{2p}$, to give $x^{p(p+1)} = x^{2p}y^{2p^2} = x^{2p^2+2p}$. This last relation reduces to $x^{p(p+1)} = 1$ which, implies $x^{8\lambda p+2p} = x^{2p} = 1$, and so $y^{2p} = 1$.

Case II $p = 8\lambda - 1$

We first examine the relation $y^{-4}(yx^2)^4y^{2p} = 1$ of $\mathcal{P}$. Using Lemmas 3.8 and 3.10 we deduce $y^{6p}(y^px^2)^4 = 1$, i.e. $xy^px^2y^px = x^{-1}y^{-p}x^{-2}y^{-p}x^{-1}y^{2p}$. As we did in Case I we proceed to examine the relation $x^p = (y^pxy^px^2)^3$ of $\mathcal{P}$. Use Lemma 3.11 and multiply by y^{2p} to obtain

$$\begin{aligned}
x^p &= y^pxy^px^2y^pxy^px^2y^pxy^px^2, \\
y^{-p}x^p &= xy^px^2y^pxy^px^2y^pxy^px^2, \\
y^{-p}x^py^{-p}x &= \underline{xy^px^2y^pxy^px^2y^pxy^px^2y^{-p}}x, \\
y^{-p}x^py^{-p}x &= x^{-1}y^{-p}x^{-2}y^{-p}x^{-1}y^{2p}y^px^2y^pxy^px^2y^{-p}x, \\
y^{2p}y^{-p}x^py^{-p}x &= y^{2p}x^{-1}\underline{y^{-p}}x^{-2}y^{-p}x^{-1}\underline{y^{2p}}y^px^2\underline{y^p}xy^px^2y^{-p}x, \\
y^{-p}x^py^px &= y^{2p}x^{-1}\underline{y^{p+6p}}x^{-2}y^{-p}x^{-1}\underline{y^{-6p}}y^px^2\underline{y^{-p-6p}}xy^px^2y^{-p}x, \\
y^{-p}x^py^px &= y^{2p-6p-6p-6p}x^{-1}y^px^{-2}y^{-p}x^{-1}y^px^2y^{-p}xy^px^2y^{-p}x, \\
y^{-p}x^py^px &= y^{-16p}x^{-1}y^px^{-2}y^{-p}x^{-1}y^px^2y^{-p}xy^px^2y^{-p}x, \\
y^{-p}x^py^px &= (x^{-1}y^px^{-2}y^{-p}x^{-1}y^p)x^2(y^{-p}xy^px^2y^{-p}x).
\end{aligned}$$

Again we raise this to the power p and use Lemma 3.7 to give $(y^{-p}x^py^px)^p = x^{2p}$. Using the fifth relation of $\mathcal{P}$ we have $(x^py^{-2p}x)^p = x^{2p}$. Now using Lemma 3.11 we get $(x^{p+1}y^{2p})^p = x^{2p}$, but since from Lemma 3.8 we have $[x^2, y^2] = 1$ we can write the last relation as $x^{p(p+1)}y^{2p^2} = x^{2p}$. On substituting $p = 8\lambda - 1$ into (5.4), and using Lemmas 3.7 and 3.10, we get $x^{2p} = 1$. So $x^{p(p+1)}y^{2p^2} = x^{2p}$ is now $y^{2p^2} = 1$, but, since $y^{8p} = 1$, we must have $y^{2p} = 1$.

Case III $p = 8\lambda + 3$

Now relation (5.4) together with Lemmas 3.7 and 3.10 gives $y^{4p} = x^{2p}$. The previous argument proved the general relation $x^{p(p+1)}y^{2p^2} = x^{2p}$. Now this is equivalent to $x^{p(p+1)} = x^{2p}y^{-2p^2} = y^{4p}y^{-2p^2} = y^{2p(2-p)}$. Since $p = 8\lambda + 3$ this last relation becomes $y^{2p} = 1$.

Case IV $p = 8\lambda + 5$

In this case $y^{3p(p+1)} = x^{2p^2}$ becomes $y^{2p} = x^{2p}$. With this last relation we may use the arguments of **Case I** to obtain the relation $x^{p(p+1)} = 1$ and with $p = 8\lambda + 5$ this is $1 = x^{p(8\lambda+6)} = x^{6p} = x^{2p}$ so $y^{2p} = 1$.

Combining **Cases I - IV** we therefore have that $G(p)^2$ is efficient on a minimal generating set. □

4 The efficiency of $G(p)^3$, p an odd prime

In this section we prove that $G(p)^3$ has an efficient presentation on a minimal generating set. After failing to find a minimal presentation using the methods of Section 2 we tried a different approach. We first need to know the Schur multiplier of $G(p)^3$.

Lemma 4.1 $M(G(p)^3) \cong C_2^6$.

Proof. We use the Schur-Künneth formula, so

$$\begin{aligned} M(G(p)^3) &\cong M(G(p)^2) \times M(G(p)) \times (G(p)^2 \otimes G(p)), \\ &\cong M(G(p)^2) \times M(G(p)) \times (G(p)^2/G(p)^{2\prime} \otimes G(p)/G(p)'), \\ &\cong C_2^3 \times C_2 \times (C_2^2 \otimes C_2), \\ &\cong C_2^3 \times C_2 \times ((C_2 \otimes C_2) \times (C_2 \otimes C_2)), \\ &\cong C_2^6. \end{aligned}$$

□

Remark 4.2 We could have used the results from Lemma 2.12 to show that $\text{rank}(M(G(p)^3)) = 3 + \begin{pmatrix} 3 \\ 2 \end{pmatrix} = 6$.

We will also need to use the following result from [73] that says

Theorem 4.3 (Lemma 4.1 of [73]) *Let H be a group, A a central subgroup of finite index, $G = H/A$. Then $H' \cap A$ is an epimorphic image of $M(G)$.*

The key idea of this section comes from Lemma 3.1 of [20], which we will reproduce here, with proof, for completeness.

Lemma 4.4 (Lemma 3.1 of [20]) *Let G be a group and let a, b, $c \in G$ satisfy the relations*

$$a(ab^{-1})^2 = 1, c^\gamma = (c^k ab^{-1})^6$$

where $\gamma = \pm 1$ and k is an integer. Then $\langle a, b, c \rangle$ is cyclic and the relations $b^2 = a^3 = c^{(6k-\gamma)}$ hold in G.

Proof. The relation $a(ab^{-1})^2 = 1$ gives $a = (ab^{-1})^{-2}, b = (ab^{-1})^{-3}$. Also $\langle a, b \rangle = \langle ab^{-1} \rangle$ and $\langle c, ab^{-1} \rangle = \langle c^k ab^{-1} \rangle$. Thus $\langle a, b, c \rangle$ is cyclic. Now the relation $c^\gamma = (c^k ab^{-1})^6$ gives $c^{\gamma - 6k} = (ab^{-1})^6$ and the result follows. □

We find a presentation for $G(p)^3$ using methods similar to those of [20].

Lemma 4.5 *If I is the group given by the presentation*

$$\langle\, a,\ b \ \mid\ a^2 = b^p = (abab^2)^3 = s,$$
$$(ab^2)^4 = t : \textit{ where } s \textit{ and } t \textit{ are central involutions} \,\rangle$$

where $p \geq 5$ then $s = t$.

Proof. The relations $b^p a^2 = 1$ and $(abab^2)^3 b^p = 1$ can easily be seen to hold in I. Now $(ab^2)^4 = t$ is equivalent to $bab^2ab = tb^{-1}a^{-1}b^{-2}a^{-1}b^{-1}$ since t is central. Substitute the last relation into $(abab^2)^3 b^p = 1$ to give

$$\begin{aligned} 1 &= abab^2\underline{ab}ab^2abab^2b^p, \\ 1 &= atb^{-1}a^{-1}b^{-2}a^{-1}b^{-1}ab^2abab^2b^p, \\ b^{-p}t &= (b^{-1}a^{-1}b^{-2}a^{-1}b^{-1})ab^2abab^2a. \end{aligned}$$

Now a^2 is a central involution and so we have

$$(b^{-1}a^{-1}b^{-2}a^{-1}b^{-1}a^{-1})b^2(abab^2ab) = a^{-2}b^{1-p}t = bt \tag{5.5}$$

since $b^p a^2 = 1$. Raising (5.5) to the power p gives $b^{2p} = b^p t$ and so $b^p = t$. Thus $s = t$. □

Lemma 4.6 *Let $J(p)$, p a prime ≥ 5, be the group defined by the presentation*

$$\begin{aligned} \langle\, a,\, b,\, u,\, v,\, x,\, y \;\mid\; & (xyxy^2)(xyxy^2a^{-1})^2,\ v^\varepsilon(v^{(p-\varepsilon)/6}xyxy^2a^{-1})^6, \\ & (uvuv^2)(uvuv^2x^{-1})^2,\ b^\varepsilon(b^{(p-\varepsilon)/6}uvuv^2x^{-1})^6, \\ & (abab^2)(abab^2u^{-1})^2,\ y^\varepsilon(y^{(p-\varepsilon)/6}abab^2u^{-1})^6, \\ & (xyxy^2)(xyxy^2u^{-1})^2,\ b^\varepsilon(b^{(p-\varepsilon)/6}xyxy^2u^{-1})^6, \\ & (ab^2)^{-4}(xy^2)^4(uv^2)^4, \\ & [a,y],\ [v,x],\ [a,u],\ [a,x], \\ & [u,x],\ [b,v],\ [b,y],\ [v,y]\,\rangle, \end{aligned}$$

where $p \equiv \varepsilon$ mod(3) and $\varepsilon \in \{-1, 1\}$. Then $J(p)$ is isomorphic to $G(p)^3$.

Proof. The proof is similar to the proof of Theorem 3.2 in [20]. Let $H = \langle a, b\rangle$, $K = \langle x, y\rangle$, and $L = \langle u, v\rangle$. By Lemma 4.4, and the fact that any missing commutators have been added in the final eight relations, we have $[H, K] = [H, L] = [K, L] = 1$ and the following relations holding in $J(p)$:

$$a^2 = b^p = (abab^2)^3 = u^2 = v^p = (uvuv^2)^3 = x^2 = y^p = (xyxy^2)^3.$$

Let $D = \langle a^2, (ab^2)^4, (xy^2)^4 \rangle$. Obviously $J(p)/D \cong G(p)^3$ and we also have $D \leqslant Z(J(p))$. To see this last assertion note that firstly a^2 is obviously central by the previous list of equalities, secondly $(ab^2)^4$ and $(xy^2)^4$ are central since $(ab^2)^{-4}(xy^2)^4(uv^2)^4 = 1$ gives $(ab^2)^4 = (xy^2)^4(uv^2)^4$ and so $(ab^2)^4$ is central and an analogous argument shows that $(xy^2)^4$ is central in $J(p)$. So by Theorem 4.3, D is a homomorphic image of $M(G(p)^3) \cong C_2^6$. By Lemma 4.5 we have $a^2 = (ab^2)^4$, $u^2 = (uv^2)^4$, $x^2 = (xy^2)^4$ but we also have $a^2 = u^2 = x^2$ and so by the ninth relation of the presentation for $J(p)$ we have $a^{-2}u^2x^2 = a^{-2}a^2a^2 = a^2 = 1$ and so D is the trivial group, and hence $J(p) \cong G(p)^3$. □

We can now proceed to the main result of this section.

Theorem 4.7 *For p a prime ≥ 5, $G(p)^3$ has an efficient presentation on a minimal generating set.*

Proof. Let ε be defined as in Lemma 4.6. We use the transformations $\alpha = v^{(p-\varepsilon)/6}xyxy^2a^{-1}$, $\beta = b^{(p-\varepsilon)/6}uvuv^2x^{-1}$, and $\gamma = y^{(p-\varepsilon)/6}abab^2u^{-1}$ to obtain $v = \alpha^{-6\varepsilon}$. Thus $xyxy^2a^{-1} = \alpha^{\varepsilon p}$, and the first relation of the presentation for $J(p)$ gives $xyxy^2 = \alpha^{-2\varepsilon p}$ and so $a = \alpha^{-3\varepsilon p}$. The other generators of $J(p)$ are obtained using a similar argument. We now transform the presentation of $J(p)$ to get

$$\begin{aligned}\mathcal{M}(p) = \langle\, \alpha,\ \beta,\ \gamma \ \mid\ & \alpha^{-2\varepsilon p}(\alpha^{-2\varepsilon p}\gamma^{3\varepsilon p})^2,\ \beta^{-6}(\beta^{1-\varepsilon p}\alpha^{-2\varepsilon p}\gamma^{3\varepsilon p})^6,\\ & (\alpha^{-3\varepsilon p}\beta^{-12\varepsilon})^{-4}(\beta^{-3\varepsilon p}\gamma^{-12\varepsilon})^4(\gamma^{-3\varepsilon p}\alpha^{-12\varepsilon})^4,\\ & [\alpha^{-3\varepsilon p}, \gamma^{-6\varepsilon}],\ [\alpha^{-6\varepsilon}, \beta^{-3\varepsilon p}],\ [\alpha^{-3\varepsilon p}, \gamma^{-3\varepsilon p}],\\ & [\alpha^{-3\varepsilon p}, \beta^{-3\varepsilon p}],\ [\beta^{-3\varepsilon p}, \gamma^{-3\varepsilon p}],\ [\alpha^{-6\varepsilon}, \beta^{-6\varepsilon}],\\ & [\beta^{-6\varepsilon}, \gamma^{-6\varepsilon}],\ [\alpha^{-6\varepsilon}, \gamma^{-6\varepsilon}]\,\rangle.\end{aligned}$$

Now the third commutator relation $[\alpha^{-3\varepsilon p}, \gamma^{-3\varepsilon p}] = 1$, on writing $p = 2\lambda + 1$, can be written as $[\alpha^{-3\varepsilon p}, \gamma^{-6\varepsilon\lambda - 3\varepsilon}] = 1$. Using the first commutator relation this implies that $[\alpha^{-3\varepsilon p}, \gamma^{-3\varepsilon}] = 1$. This last relation implies the first and third

commutator relations, and in turn is implied by the first and third commutator relations of $\mathcal{M}(p)$ and so we can replace two of the relations in $\mathcal{M}(p)$ with a single relation. Using the last argument we can replace the second and fourth relations of $\mathcal{M}(p)$ with a single relation. Now our presentation is

$$\begin{aligned}\langle\, \alpha,\ \beta,\ \gamma \ \mid\ & \alpha^{-2\varepsilon p}(\alpha^{-2\varepsilon p}\gamma^{3\varepsilon p})^2,\ \beta^{-6}(\beta^{1-\varepsilon p}\alpha^{-2\varepsilon p}\gamma^{3\varepsilon p})^6,\\ & (\alpha^{-3\varepsilon p}\beta^{-12\varepsilon})^{-4}(\beta^{-3\varepsilon p}\gamma^{-12\varepsilon})^4(\gamma^{-3\varepsilon p}\alpha^{-12\varepsilon})^4,\\ & [\alpha^{-3\varepsilon p},\gamma^{-3\varepsilon}],\ [\alpha^{-3\varepsilon},\beta^{-3\varepsilon p}],\\ & [\beta^{-3\varepsilon p},\gamma^{-3\varepsilon p}],\ [\alpha^{-6\varepsilon},\beta^{-6\varepsilon}],\\ & [\beta^{-6\varepsilon},\gamma^{-6\varepsilon}],\ [\alpha^{-6\varepsilon},\gamma^{-6\varepsilon}]\,\rangle.\end{aligned}$$

This presentation has deficiency six, and so is an efficient presentation for $G(p)^3$, p a prime ≥ 5, on a minimal generating set. □

We now give a presentation for $G(3)^3$ to complete the requirement that $G(p)$ be efficient for all odd primes p.

Lemma 4.8 *$G(3)^3$ has the following as an efficient presentation on a minimal generating set:*

$$\begin{aligned}\langle\, \alpha,\ \beta,\ \gamma \ \mid\ & \alpha^{-4}(\alpha\beta^2)^4\beta^6,\ \beta^{-4}(\beta\gamma^2)^4\gamma^6\alpha^6,\ \gamma^{-4}(\gamma\alpha^2)^4,\\ & \beta^{-3}(\alpha^3\beta\alpha^3\beta^2)^3,\gamma^{-3}(\beta^3\gamma\beta^3\gamma^2)^3,\ \alpha^{-3}(\gamma^3\alpha\gamma^3\alpha^2)^3,\\ & [\alpha^3,\gamma]\alpha^6,\ [\beta^3,\alpha],\ [\gamma^3,\beta]\,\rangle.\end{aligned}$$

Proof. This may be verified using a Todd-Coxeter program. We used the ACE package in GAP [36]. □

We are now in a position to prove the main result of this chapter.

Theorem 4.9 *Direct powers of the group $G(p)$ (p an odd prime) are efficient. In particular when $x^2 \equiv 2 \bmod p$ has no integer solutions then direct powers of $PGL(2,p)$ are efficient.*

Proof. This follows from Theorems 2.8, 3.12, 4.7, Corollary 2.15 and Lemma 4.8. □

Note Appendix A gives a list of all primes p, $p < 1000$, and identifies when the congruence $x^2 \equiv 2 \bmod p$ has no integer solutions. This is equivalent to $p \equiv \pm 1 \bmod 8$.

Chapter 6

An efficient presentation for $PGL(2,p)$ and a related group

1 Introduction

In this chapter we present a presentation for the group $PGL(2,p)$, where p is an odd prime. The given presentation will define $PGL(2,p)$ on a minimal generating set. This presentation will depend on finding a primitive root in $GF(p)$ that satisfies certain conditions. Theorems and conjectures concerning the existence of such a primitive root are also presented. Examples of such primitive roots are given in Appendix A. We then present presentations for $PGL(2,p) \times PGL(2,p)$.

2 Background

The general linear group of $n \times n$ non-singular matrices over the field with p elements, p a prime, denoted by $GL(n,p)$ has, as a quotient group, $PGL(n,p)$ defined as

Definition 2.1 The *projective general linear group* of $n \times n$ matrices over the field with p elements, p a prime, written as $PGL(n,p)$ is the factor group $GL(n,p)/Z(GL(n,p))$.

The centre of $GL(n,p)$ is the set of diagonal matrices

$$\begin{pmatrix} a & 0 & \dots & 0 \\ & \ddots & & \\ 0 & \dots & a & 0 \\ 0 & \dots & 0 & a \end{pmatrix}$$

where $a \in \mathbb{Z}_p^*$, the multiplicative group of order $p-1$.

It will be useful to know the order of $PGL(n,p)$, and hence we have:

Lemma 2.2 *The order of* $PGL(n,p)$ *is* $(p^n-1)(p^n-p)\dots(p^n-p^{n-1})/(p-1)$.

Proof. We first show that $|GL(n,p)| = (p^n-1)(p^n-p)\dots(p^n-p^{n-1})$. To see this we examine the possible rows of elements from $GL(n,p)$. The first row has p^n-1 possibilities, we exclude the row containing just zeros. The next row has p^n-p possibilities, no multiplication of the first row being allowed. This argument continues, giving $|GL(n,p)| = (p^n-1)(p^n-p)\dots(p^n-p^{n-1})$.

The centre of $GL(n,p)$ has order $p-1$ and hence the result follows. □

In [55] it was claimed that $PGL(2,p)$ is efficient. The authors proposed the following presentation for $PGL(2,p)$:

$$\langle\, x, y \;\mid\; x^2 = 1, y^p = 1, (xy^2xy^r)^2 = 1, (xyxy^r)^3 = 1 \,\rangle$$

where r is a primitive element of $GF(p)$.

It was also claimed that letting $r = 2$ will also yield a presentation for $PGL(2,p)$. From this presentation the authors obtained the following efficient

presentation which it was claimed was an efficient presentation for $PGL(2,p)$ on a minimal generating set

$$\langle\, x, y \;\mid\; x^2y^p = 1, (xy^2)^4 = 1, (xyxy^2)^3y^p = 1 \,\rangle.$$

Unfortunately the analysis used to obtain this presentation inherited an error from a presentation for $PSL(2,p)$ that was used in the derivation of the above. In fact it has been shown that

Theorem 2.3 *Let p be an odd prime. If $x^2 \equiv 2 \bmod p$ has no solutions in the integers the presentation*

$$\langle\, x, y \;\mid\; x^2y^p = 1, (xy^2)^4 = 1, (xyxy^2)^3y^p = 1 \,\rangle$$

defines a group isomorphic to $PGL(2,p)$.

Proof. See [40]. □

The smallest example when the above presentation fails to define $PGL(2,p)$ is when $p = 7$.

Example 2.4 Let $p = 7$ in the above presentation. The equation $x^2 \equiv 2 \bmod 7$ has a solution since $1 = (\frac{2}{7}) \equiv 2^{(7-1)/2} \bmod 7$, where (-) is the Legendre symbol. Now the presentation

$$\mathcal{P} = \langle\, x, y \;\mid\; x^2y^7 = 1, (xy^2)^4 = 1, (xyxy^2)^3y^7 = 1 \,\rangle$$

does not define $PGL(2,7)$ since if we let P denote the group defined by $\mathcal{P}$ we have the following group invariants:

Group Invariant	P	$PGL(2,7)$
Exponent	84	168
Number of normal subgroups	4	3
ϕ_2	57456	69552
ϕ_3	31441536	32570496

The exponent, ex, of a group G is taken to be the lowest common multiple of the orders of its elements, so for any $g \in G$, $g^{ex} = 1$.

It can be shown that the group defined by the presentation $\mathcal{P}$ is isomorphic to the group $PSL(2,7) \times C_2$.

3 An efficient presentation for $PGL(2,p)$, p and odd prime

Here we present a new presentation that defines $PGL(2,p)$ for all odd primes p, with the exceptions of $3, 5$ and possibly a finite number of primes. Our new presentation will depend on one found in [55] that always defines $PGL(2,p)$.

Before we give the presentation and its proof we need the following results.

Theorem 3.1 *The Schur multiplier of $PGL(2,p)$ where p is an odd prime, written $M(PGL(2,p))$, is the cyclic group of order two.*

Proof. See [43]. □

Lemma 3.2 *The group $PGL(2,p)/PGL(2,p)'$ is isomorphic to the cyclic group of order two.*

Proof. The following presentation always defines the group $PGL(2,p)$

$$\langle\, x, y \;\mid\; x^2 = 1, y^p = 1, (xy^2xy^r)^2 = 1, (xyxy^r)^3 = 1 \,\rangle$$

where r is an odd primitive root of $GF(p)$, with p an odd prime. Using the relation matrix method on this presentation the result follows.

Alternatively it is a well known result that $PGL(2,p)/PGL(2,p)' \cong C_2$ and this result may be quoted. □

We now need to find special primitive roots in $GF(p)$. The reason for this will become apparent later on.

Lemma 3.3 *Let p be an odd prime, $p > 5$. The field $GF(p)$ contains an odd primitive root r that satisfies $(p-3, r-4) = 1$, where either $p < 10^8$ or $p > 10^{20}$.*

Proof. Let $p > 5$ be an odd prime.

The fact that $GF(p)$ contains an odd primitive root that satisfies $(p-3, r-4) = 1$ for $p < 10^8$ has been checked using the GAP computational algebra system [36].

In [27] it was shown that the field $GF(p)$ contain an odd primitive root satisfying $(p-3, r-4) = 1$ if

$$\phi(p-3) > W^{(p-1)(p-3)}\sqrt{p}\log p$$

where $W(m) = 2^{\omega(m)}$ is the number of square-free divisors of m. This is guaranteed to hold for $p > 10^{20}$. □

Our computer search is not very satisfying as we are not able to use any of the efficient polynomial time search algorithms, see [8], due to our extra restrictions.

By the prime number theorem Lemma 3.3 has not been able to consider $\pi(10^{20}) - \pi(10^8) \approx 2.1714 \times 10^{18}$ primes. If one of these primes does not have the required properties then this would have to be investigated further as this prime will be one of a 'small' number of exceptions and it would be interesting to find out why.

We now give the main result of this section

Theorem 3.4 *Let $p > 5$, p an odd prime, and r be an odd primitive root of $GF(p)$ satisfying $(p-3, r-4) = 1$, if one exists. Under these circumstances the*

presentation

$$\mathcal{P} = \langle\, a, b \;\mid\; a^2b^{2p} = 1, (ab^2ab^r)^2 = 1, (ababb^r)^3b^p = 1 \,\rangle$$

defines $PGL(2,p)$.

Proof. Let p be an odd prime, $p > 5$, and let r be a primitive root of $GF(p)$ satisfying $(p-3, r-4) = 1$. Let $G_{p,r}$ be the group defined by the presentation

$$\langle\, a, b \;\mid\; a^2b^{2p} = 1, (ab^2ab^r)^2 = 1, (ababb^r)^3b^p = 1 \,\rangle.$$

Obviously a^2 and b^{2p} are both contained in the centre of $G_{p,r}$. Also in the group $G_{p,r}/G'_{p,r}$ the following hold

$$a^2b^{2p} = 1,\ a^4b^{2r+4} = 1,\ a^6b^{p+3r+3} = 1.$$

The second and third relations together give $a^2b^{p+r-1} = 1$. When this last relation is combined with $a^2b^{2p} = 1$ we obtain $b^r = b^{p+1}$. Using this last equation the three expressions above become:

$$a^2b^{2p} = 1,\ a^4b^{2p+6} = 1,\ a^6b^{4p+6} = 1.$$

The first and the second expressions above give $a^2b^6 = 1$. We have $a^2b^{2p} = 1$ and $a^2b^6 = 1$, which together give $b^{2p} = b^6$. Now the order of b is $(p+r-7, r-p-1, 2p-6) = (p-3, r-4)$ which we require to be one and hence the greatest common divisor condition in the statement of the theorem. So we have $a^2b^{2p} = 1$ or $a^2 = 1$. So since $a^2 = 1$ in $G_{p,r}/G'_{p,r}$, and a^2 is in the centre of $G_{p,r}$, we have $a^4 = 1$ in the group $G_{p,r}$.

Now we consider the group $G_{p,r}$.

We have $a^2 = b^{-2p}$, so $1 = a^4 = b^{-4p}$. Thus $1 = b^{4p}$. From $(ab^2ab^r)^2 = 1$ we obtain $babab^rab = b^{-1}a^{-1}b^{-r}a^{-1}b^{-1}$. From $(ababb^r)^3b^p = 1$ we see that b^p commutes

with $abab^r$. Now the third relation is

$$\begin{aligned} 1 &= abab^r abab^r abab^r \underline{b^p} \\ &= \underline{a}bab^r abab^{r+p} abab^r \\ &= \underline{bab^r ab}ab^{r+p} abab^r a. \end{aligned}$$

Now use the expression $bab^r ab = b^{-1}a^{-1}b^{-r}a^{-1}b^{-1}$ to give

$$1 = b^{-1}a^{-1}b^{-r}a^{-1}b^{-1}ab^{r+p}abab^r a.$$

Because $a^4 = 1$ and $a^2 \in Z(G_{p,r})$ we obtain

$$\begin{aligned} \underline{ba^{-2}} &= a^{-1}b^{-r}a^{-1}b^{-1}a^{-1}b^{r+p}abab^r a \\ b^{2p+1} &= (abab^r a)^{-1}b^{p+r}(abab^r a). \end{aligned}$$

Now raise the above to the power p and use the facts that $p + r$ is even and $b^{2p} \in Z(G_{p,r})$ to give:

$$\begin{aligned} b^{p(2p+1)} &= b^{p(p+r)} \\ &= b^p a^{-2p}, \end{aligned}$$

which gives $b^{p(p+r-1)} = b^{2p^2}$, giving $b^{p(r-p-1)} = 1$. We now note that $r - p - 1$ is odd and so $(p(r-p-1), 4p) = p$. Thus $b^p = 1$. So the presentation $\mathcal{P}$ s equivalent to the presentation

$$\langle\, a, b \;\mid\; a^2 = 1, b^p = 1, (ab^2ab^r)^2 = 1, (abab^r)^3 = 1 \,\rangle,$$

the known presentation for $PGL(2,p)$. □

So we may say:

Theorem 3.5 *Let p be a prime. The group $PGL(2,p)$ is efficient on a minimal generating set (with possibly a finite number of exceptions).*

Proof. The last theorem dealt with all primes p, $p > 5$ (assuming that there exists a primitive root r satisfying $(p-3, r-4) = 1$).

Since $|PGL(2,2)| = 6$ we know that $PGL(2,2) \cong D_{2(3)}$ and an efficient presentation for $D_{2(3)}$ on a minimal generating set is:

$$\langle\, a, b \;\mid\; a^2 = 1, b^3 = 1, (ab)^2 = 1 \,\rangle.$$

Also $|PGL(2,3)| = 24$ and we have $PGL(2,3) \cong S_4$. An efficient presentation for S_4 on a minimal generating set is

$$\langle\, a, b \;\mid\; a^4 = 1, b^2 = 1, (ab)^3 = 1 \,\rangle.$$

The presentation

$$\langle\, a, b \;\mid\; a^2b^5 = 1, (ab^2)^4 = 1, (abab^2)^3b^5 = 1 \,\rangle$$

defines $PGL(2,5)$.

Thus the result of the theorem holds. □

4 On a presentation for the group $PGL(2,p) \times PGL(2,p)$

In this section we construct presentations for $PGL(2,p) \times PGL(2,p)$ based on the presentation

$$\langle\, a, b \;\mid\; a^2 = 1, b^p = 1, (ab^2ab^r)^2 = 1, (abab^r)^3 = 1 \,\rangle$$

where r is an odd primitive root in $GF(p)$, p an odd prime. We may always find an odd primitive root in $GF(p)$, $p > 3$, by a result of S. D. Cohen; see [25].

We start by using the above presentation to give a 'standard' presentation for $PGL(2,p) \times PGL(2,p)$.

Lemma 4.1 *Let p be an odd prime and r an odd primitive root in $GF(p)$. The group $PGL(2,p) \times PGL(2,p)$ can be presented by:*

$$\langle\, u, v | v^{2p}, u^{2p}, (v^p u^2 v^p u^r)^2, (v^p u v^p u^r)^3, (u^p v^2 u^p v^r)^2, (u^p v u^p v^r)^3, [u^p, v^p], [u^2, v^2] \,\rangle.$$

Proof. We first give the 'standard' presentation for the direct product $PGL(2,p) \times PGL(2,p)$:

$$\begin{aligned} \langle\, a, b, c, d \;\mid\; & a^2 = 1, b^p = 1, (ab^2ab^r)^2 = 1, (abab^r)^3 = 1, \\ & c^2 = 1, d^p = 1, (cd^2cd^r)^2 = 1, (cdcd^r)^3 = 1, \\ & [a,c] = 1, [a,d] = 1, [b,c] = 1, [b,d] = 1 \,\rangle. \end{aligned}$$

Now we introduce two new generators u and v defined as $u = ad$ and $v = bc$. From the relations $a^2 = 1$ and $d^p = 1$ we have $u^{2p} = 1$ and $u^p = a$ so $d = u^{1-p}$. Likewise we have $c = v^p$ and $b = v^{1-p}$. Now we list the relations from the above 'standard' presentation and rewrite them in terms of u and v:

$$\begin{aligned} a^2 = 1 &\longrightarrow u^{2p} = 1, \\ b^p = 1 &\longrightarrow v^{p(1-p)} = 1, \\ (ab^2ab^r)^2 = 1 &\longrightarrow (u^p v^{2(1-p)} u^p v^{r(1-p)})^2 = 1, \\ (abab^r)^3 = 1 &\longrightarrow (u^p v^{(1-p)} u^p v^{r(1-p)})^3 = 1, \\ c^2 = 1 &\longrightarrow v^{2p} = 1, \\ d^p = 1 &\longrightarrow u^{p(1-p)} = 1, \\ (cd^2cd^r)^2 = 1 &\longrightarrow (v^p u^{2(1-p)} v^p u^{(1-p)})^2 = 1, \\ (cdcd^r)^3 = 1 &\longrightarrow (v^p u^{(1-p)} v^p u^{r(1-p)})^3 = 1, \\ [a,c] = 1 &\longrightarrow [u^p, v^p] = 1, \\ [a,d] = 1 &\longrightarrow [u^p, u^{1-p}] = 1, \\ [b,c] = 1 &\longrightarrow [v^{1-p}, v^p] = 1, \\ [b,d] = 1 &\longrightarrow [v^{1-p}, u^{1-p}] = 1. \end{aligned}$$

Now $u^{2p} = 1$ implies $u^{p(1-p)} = 1$, and likewise $v^{2p} = 1$ implies $v^{p(1-p)} = 1$.

Obviously $[u^p, u^{1-p}] = 1$ and $[v^{1-p}, v^p] = 1$ can be removed from the presentation.

The two commutators $[u^p, v^p] = 1$ and $[v^{1-p}, u^{1-p}] = 1$ reduce to $[u^p, v^p] = 1$ and $[v^2, u^2] = 1$ as follows:

$$\begin{aligned} [v^{1-p}, u^{1-p}] &= [v^{1-p}, u^{1+p}], \text{ since } u^{2p} = 1, \\ [v^{1-p}, u^{1-p}] &= [v^{1-p}, u^{1-p}u^{1+p}], \\ [v^{1-p}, u^{1-p}] &= [v^{1-p}, u^2]. \end{aligned}$$

An analogous result holds to show that $[v^{1-p}, u^2] = [v^2, u^2]$.

We also note that $1 = (u^p v^{2(1-p)} u^p v^{r(1-p)})^2 = (u^p v^2 u^p v^{r-p})^2$ and, since $[u^p, v^p] = 1$ and $v^{2p} = 1$, we get $(u^p v^2 u^p v^{r-p})^2 = (u^p v^2 u^p v^r)^2 = 1$. Likewise we have $1 = (v^p u^{2(1-p)} v^p u^{r(1-p)})^2 = (v^p u^2 v^p u^r)^2$.

Noting r is odd and $[u^p, v^p] = 1$ we have

$$\begin{aligned} 1 &= (v^p u^{(1-p)} v^p u^{r(1-p)})^3 \\ &= (v^p u^{(1-p)} v^p u^{r-p})^3 \\ &= (v^p u v^p u^r)^3. \end{aligned}$$

Again an analogous argument shows that $(u^p v u^p v^r)^3 = 1$.

Thus the results holds. □

Now we have a presentation for $PGL(2,p) \times PGL(2,p)$ we may calculate the abelian invariants of this group.

Lemma 4.2 *Let P be the group defined by the presentation*

$$\langle u, v | v^{2p}, u^{2p}, (v^p u^2 v^p u^r)^2, (v^p u v^p u^r)^3, (u^p v^2 u^p v^r)^2, (u^p v u^p v^r)^3, [u^p, v^p], [u^2, v^2] \rangle.$$

The group $(P \times P)/(P \times P)'$, where p is an odd prime, is isomorphic to the group $C_2 \times C_2$.

Proof. We first write down the relation matrix of the presentation:

$$\begin{pmatrix} 2p & 0 \\ 0 & 2p \\ 4+2r & 4p \\ 3+3r & 6p \\ 4p & 4+2r \\ 6p & 3+3r \end{pmatrix} \longrightarrow \begin{pmatrix} 2p & 0 \\ 0 & 2p \\ 4+2r & 0 \\ 3+3r & 0 \\ 0 & 4+2r \\ 0 & 3+3r \end{pmatrix}$$

$$\longrightarrow \begin{pmatrix} 2p & 0 \\ 0 & 2p \\ 1-r & 0 \\ 0 & 0 \\ 0 & 1-r \\ 0 & 0 \end{pmatrix}$$

$$\longrightarrow \begin{pmatrix} 2 & 0 \\ 0 & 2 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Thus the group $(P \times P)/(P \times P)'$ is isomorphic to the group $C_2 \times C_2$. □

Knowing about the group $PGL(2,p)/PGL(2,p)'$ gives us information about the Schur multiplier of $PGL(2,p) \times PGL(2,p)$ as the following shows:

Lemma 4.3 *The Schur multiplier of the group $PGL(2,p)^2$ is isomorphic to C_2^3.*

Proof. To show this we use the Schur-Künneth formula:

$$\begin{aligned} M(PGL(2,p)^2) &\cong M(PGL(2,p)) \times M(PGL(2,p)) \times (PGL(2,p) \otimes PGL(2,p)), \\ &\cong M(PGL(2,p)) \times M(PGL(2,p)) \\ &\quad \times (PGL(2,p)/PGL(2,p)' \otimes PGL(2,p)/PGL(2,p)'), \\ &\cong C_2 \times C_2 \times (C_2 \otimes C_2), \\ &\cong C_2^3. \end{aligned}$$

Thus the result holds. □

So now if something can be shown to be in the multiplier we may deduce that it has order two. We will use this fact in some of the following proofs.

We now show that some of the relations in the above presentation for $PGL(2,p)^2$ can be omitted and the resulting presentation will still define the same group.

Lemma 4.4 *In the presentation*

$$\langle\, u, v | v^{2p}, u^{2p}, (v^p u^2 v^p u^r)^2, (v^p u v^p u^r)^3, (u^p v^2 u^p v^r)^2, (u^p v u^p v^r)^3, [u^p, v^p], [u^2, v^2] \,\rangle,$$

where p is an odd prime and r is an odd primitive root in $GF(p)$, the relation $v^{2p} = 1$ can be omitted and the group defined by the resulting presentation will be $PGL(2,p)^2$.

Proof. Let $\mathcal{P}_{p,r}$ be the presentation defined by

$$\langle\, u, v | u^{2p}, (v^p u^2 v^p u^r)^2, (v^p u v^p u^r)^3, (u^p v^2 u^p v^r)^2, (u^p v u^p v^r)^3, [u^p, v^p], [u^2, v^2] \,\rangle,$$

where p is an odd prime and r is an odd primitive root in $GF(p)$.

Since $[u^p, v^p] = 1$ and $[u^2, v^2] = 1$ in $\mathcal{P}_{p,r}$ we may deduce that v^{2p} is central. It is easy to see that $v^{2p} = 1$ in $\mathcal{P}_{p,r}/\mathcal{P}'_{p,r}$. So we now know that $v^{4p} = 1$ in $\mathcal{P}_{p,r}$.

The second relation, namely $(v^p u^2 v^p u^r)^2 = 1$, gives $uv^p u^r v^p u = (uv^p u^r v^p u)^{-1}$. The third relation of $\mathcal{P}_{p,r}$ is $(v^p u v^p u^r)^3 = 1$ or equally $uv^p u^r v^p u v^p u^r v^p u v^p u^r v^p = 1$. We now replace the first $2p + r + 2$ letters with their inverse to give

$$1 \;=\; (uv^p u^r v^p u)^{-1} v^p u^r v^p u v^p u^r v^p$$

So we may say $u = (uv^p u^r v^p u)^{-1} v^p u^r v^p (uv^p u^r v^p u)$. Now raise this to the power p to give

$$\begin{aligned} u^p &= (uv^p u^r v^p u)^{-1} (\underline{v^p u^r v^p})^p (uv^p u^r v^p u), \\ &= (uv^p u^r v^p u)^{-1} \underline{u^{pr} v^{2p^2}} (uv^p u^r v^p u), \text{ since } 1 = [u^p, v^p] \text{ and } v^{2p} \text{ is central}, \\ &= u^p v^{2p^2}, \text{ since } 1 = [u^p, v^p],\ v^{2p} \text{ is central and } r \text{ is odd}. \end{aligned}$$

So $v^{2p^2} = 1$. Putting $v^{4p} = 1$ together with $v^{2p^2} = 1$ gives $v^{2p} = 1$ as required. □

We continue the process by removing another relation.

Lemma 4.5 *The presentation $\mathcal{H}_{p,r}$ given by:*

$$\langle\, u, v | (v^p u^2 v^p u^r)^2, (v^p u v^p u^r)^3 u^{2p}, (u^p v^2 u^p v^r)^2, (u^p v u^p v^r)^3, [u^p, v^p], [u^2, v^2] \,\rangle,$$

where p is an odd prime and r is an odd primitive root in $GF(p)$, defines $PGL(2,p)^2$.

Proof. To show the result we just need to show that $u^{2p} = 1$ holds in $\mathcal{H}_{p,r}$, as this together with the previous lemma will give the result.

We see that u^{2p} is central from the relations $[u^p, v^p] = 1$ and $[u^2, v^2] = 1$. It is also easy to see that $u^{2p} = 1$ in $\mathcal{H}_{p,r}/\mathcal{H}'_{p,r}$. So by the multiplier argument we obtain the relation $u^{4p} = 1$ in $\mathcal{H}_{p,r}$. Using an analogous argument we see that $v^{4p} = 1$ holds in $\mathcal{H}_{p,r}$.

Now on rewriting $1 = (v^p u^2 v^p u^r)^2$ so that it is $vu^p v^r u^p v = (vu^p v^r u^p v)^{-1}$.

Using the fourth relation we get

$$\begin{aligned} 1 &= u^p \underline{vu^pv^ru^pv} u^pv^ru^pvu^pv^r, \\ &= \underline{u^p}(vu^pv^ru^pv)^{-1}u^pv^ru^pvu^pv^r, \\ &= (vu^pv^ru^pv)^{-1}u^pv^ru^p(vu^pv^ru^p), \end{aligned}$$

so, on postmultiplying by v we get, $v = (vu^pv^ru^pv)^{-1}u^pv^ru^p(vu^pv^ru^pv)$. On raising the last equality to the power p we obtain

$$\begin{aligned} v^p &= (vu^pv^ru^pv)^{-1}\underline{(u^pv^ru^p)^p}(vu^pv^ru^pv), \\ &= (vu^pv^ru^pv)^{-1}(u^p\underline{v^{pr}}u^pu^{2p(p-1)})(vu^pv^ru^pv) \text{ since } u^{2p} \text{ is central}, \\ &= v^{pr}u^{2p^2} \text{ since } 1 = [u^p, v^p]. \end{aligned}$$

So we have $v^p = v^{pr}u^{2p^2}$. Since $p = 2\lambda + 1$, for $\lambda \in \mathbb{Z}$, we have $v^p = v^{pr}u^{2(2\lambda+1)p}$ or, since $u^{4p} = 1$, $v^p = v^{pr}u^{2p}$. Thus we are left with $v^{(1-r)p} = u^{2p}$.

Now we examine $1 - r$.

If $1 - r = 4x$, for $x \in \mathbb{Z}$, we have $u^{2p} = 1$ and the result holds.

If $(1 - r, 4) = 2$ then we have $v^{2p} = u^{2p}$. We know that the relation $1 = (u^pv^2u^pv^r)^2$ gives $uv^pu^rv^pu = (uv^pu^rv^pu)^{-1}$ so

$$\begin{aligned} 1 &= \underline{v^p}uv^pu^rv^puv^pu^rv^puv^pu^ru^{2p}, \\ &= \underline{uv^pu^rv^pu}v^pu^rv^puv^pu^ru^{2p}v^p, \\ &= (uv^pu^rv^pu)^{-1}v^pu^rv^p(uv^pu^rv^p)u^{2p}, \text{ since } 1 = [u^p, v^p]. \end{aligned}$$

This gives

$$u^{2p+1} = (uv^pu^rv^pu)^{-1}v^pu^rv^p(uv^pu^rv^pu).$$

Raising this to the power p gives

$$\begin{aligned} u^{p(2p+1)} &= (uv^pu^rv^pu)^{-1}\underline{(v^pu^rv^p)^p}(uv^pu^rv^pu), \\ &= (uv^pu^rv^pu)^{-1}(v^{2p^2}u^{pr})(uv^pu^rv^pu), \\ &= v^{2p^2}u^{pr}. \end{aligned}$$

The above is equal to $u^{p(2p+1)} = u^{p(2(2\lambda+1)+1)} = u^{3p}$, where $p = 2\lambda + 1$. So $u^{p(2p+1)} = v^{2p^2}u^{pr}$ becomes $u^{(3-r)p} = v^{2p^2}$. Now if $(1-r, 4) = 2$ then $(3-r, 4) = 4$, so $u^{(3-r)p} = 1 = v^{2p^2}$ and we have both $1 = v^{2p^2}$ and $1 = v^{4p}$ so, since p is odd, we have $1 = v^{2p}$. But $v^{2p} = u^{2p}$, so $1 = u^{2p}$ as required. □

We conclude this chapter by mentioning that if it is possible to find a presentation for $PGL(2,p)^2$ that requires two generators and five relators and a presentation for $PGL(2,p)^3$ that requires three generators and nine relators then together these results show that $PGL(2,p)^n$ is efficient, for any positive integer n. Unfortunately no such presentations have be found at this point in time.

Appendix A

Numerical results

Below is a list of all primes p_n, $1 \leq n \leq 168$, less than 1000 together with their Wall numbers, $k(p_n)$, and the smallest odd primitive root in $GF(p_n)$, denoted by $r(p_n)$, satisfying $(p_n - 3, r(p_n) - 4) = 1$.

n	p_n	$k(p_n)$	$r(p_n)$	n	p_n	$k(p_n)$	$r(p_n)$	n	p_n	$k(p_n)$	$r(p_n)$
1	2*	3	–	11	31	30	13	21	73	148	13
2	3*	8	–	12	37*	76	13	22	79	78	7
3	5*	20	–	13	41	40	7	23	83*	168	13
4	7	16	5	14	43*	88	33	24	89	44	7
5	11*	10	7	15	47	32	11	25	97	196	7
6	13*	28	7	16	53*	108	21	26	101*	50	7
7	17	36	7	17	59*	58	13	27	103	208	11
8	19*	18	13	18	61*	60	7	28	107*	72	7
9	23	48	7	19	67*	136	7	29	109*	108	11
10	29*	14	11	20	71	70	7	30	113	76	17

n	p_n	$k(p_n)$	$r(p_n)$	n	p_n	$k(p_n)$	$r(p_n)$	n	p_n	$k(p_n)$	$r(p_n)$
31	127	256	7	59	277*	556	11	87	449	448	13
32	131*	130	17	60	281	56	11	88	457	916	13
33	137	276	13	61	283*	568	17	89	461*	46	7
34	139*	46	15	62	293*	588	7	90	463	928	11
35	149*	148	11	63	307*	88	13	91	467*	936	11
36	151	50	7	64	311	310	17	92	479	478	13
37	157*	316	21	65	313	628	15	93	487	976	11
38	163*	328	7	66	317*	636	13	94	491*	490	7
39	167	336	13	67	331*	110	11	95	499*	498	7
40	173*	348	7	68	337	676	15	96	503	1008	15
41	179*	178	7	69	347*	232	7	97	509*	254	7
42	181*	90	21	70	349*	174	7	98	521	26	7
43	191	190	19	71	353	236	13	99	523*	1048	21
44	193	388	15	72	359	358	7	100	541*	90	13
45	197*	396	11	73	367	736	19	101	547*	1096	7
46	199	22	15	74	373*	748	11	102	557*	124	11
47	211*	42	7	75	379	378	7	103	563*	376	15
48	223	448	11	76	383	768	11	104	569	568	11
49	227*	456	13	77	389*	388	15	105	571*	570	17
50	229*	114	7	78	397*	796	7	106	577	1156	7
51	233	52	11	79	401	200	13	107	587*	1176	11
52	239	238	7	80	409	408	21	108	593	1188	7
53	241	240	7	81	419*	418	11	109	599	598	7
54	251*	250	11	82	421*	84	39	110	601	600	7
55	257	516	7	83	431	430	7	111	607	1216	17
56	263	176	7	84	433	868	7	112	613*	1228	11
57	269*	268	7	85	439	438	15	113	617	1236	13
58	271	270	15	86	443*	888	7	114	619*	206	19

n	p_n	$k(p_n)$	$r(p_n)$	n	p_n	$k(p_n)$	$r(p_n)$	n	p_n	$k(p_n)$	$r(p_n)$
115	631	630	7	133	751	750	17	151	877*	1756	13
116	641	640	17	134	757*	1516	15	152	881	176	15
117	643*	1288	11	135	761	380	7	153	883*	1768	11
118	647	1296	15	136	769	192	11	154	887	1776	15
119	653*	1308	21	137	773*	1548	7	155	907*	1816	7
120	659*	658	7	138	787*	1576	13	156	911	70	17
121	661*	220	23	139	797*	228	7	157	919	102	7
122	673	1348	11	140	809	202	11	158	929	928	7
123	677*	452	7	141	811*	270	13	159	937	1876	7
124	683*	1368	7	142	821*	820	11	160	941*	470	7
125	691*	138	13	143	823	1648	7	161	947*	1896	11
126	701*	700	11	144	827*	1656	7	162	953	212	11
127	709*	118	17	145	829*	276	19	163	967	176	7
128	719	718	11	146	839	838	11	164	971*	970	11
129	727	1456	19	147	853*	1708	11	165	977	652	13
130	733*	1468	7	148	857	1716	7	166	983	1968	13
131	739*	738	7	149	859*	78	29	167	991	198	7
132	743	496	7	150	863	1728	7	168	997*	1996	7

Notes: For all the primes above $k(p_n^2) = p_n k(p_n)$. Using this information and the above results we may calculate $k(m)$ where $m = \prod_{i=1}^{168} p_i^{\alpha_i}$ with $\alpha_i \in \mathbb{N} \cup \{0\}$.

An asterisk besides a prime number p_n indicates that there is no solution to the equation $x^2 \equiv 2 \bmod p_n$ and so the group defined by the presentation $\langle a, b \mid a^2, b^{p_n}, (ab^2)^4, (abab^2)^3 \rangle$ is isomorphic to $PGL(2, p_n)$; otherwise it is isomorphic to $PSL(2, p_n) \times C_2$.

Appendix B

A form for the Fibonacci orbit of D_∞^3

In this appendix we prove the following result in order to provide us with a useful working example that may be used in Chapter 4.

Lemma 0.6 *Every element of the Fibonacci orbit* $(x_j)_{j=1}^{\infty}$ *of* $D_\infty^3 = \langle a_1, b_1, a_2, b_2, a_3, b_3 \rangle$ *may be represented by:*

$$x_j = \begin{cases} a_1, & j \equiv 1, -6 \bmod 14 \\ b_1^{\pm 1}, & j \equiv 2, -5 \bmod 14 \\ a_2 b_1^{\pm 2(j-3)/7}, & j \equiv 3, -4 \bmod 14 \\ b_2^{\pm 1} b_1^{\pm 2(j-4)(j+3)/7^2}, & j \equiv 4, -3 \bmod 14 \\ a_3 b_2^{\pm 2(j-5)/7} b_1^{\pm 4(j-5)(j+2)(j+9)/(3\times 7^3)}, & j \equiv 5, -2 \bmod 14 \\ b_3^{\pm 1} b_2^{\pm 2(j+1)(j-6)/7^2} b_1^{\pm 2(j-6)(j+1)(j+8)(j+15)/(3\times 7^4)}, & j \equiv 6, -1 \bmod 14 \\ a_3 a_2 a_1 b_3^{\pm 1} b_2^{\pm (2j^2-7^2)/7^2} b_1^{\pm (2(j/7)^4+8(j/7)^3+4(j/7)^2-8(j/7)-3)/3}, & j \equiv 7,\ 0 \bmod 14 \end{cases}$$

where the positive exponent is chosen for the first value of j *and the negative exponent is chosen for the second value of* j.

Proof. We use induction on j. Firstly we note that the anchor stage holds trivially.

Now assume that the result holds for all values less than or equal to j, $j \equiv 0 \bmod 14$. We show that the next 14 consecutive values of the Fibonacci orbit follow the form of the lemma.

$$\begin{aligned}
x_{j+1} &= b_1^{-1}a_2b_1^{-2(j-7)/7}b_2^{-1}b_1^{-2(j-7)(j+3)/7^2}a_3b_2^{-2(j-7)/7}b_1^{-4(j-7)j(j+7)/(3\times 7^3)}b_3^{-1} \\
&\quad b_2^{-2j(j-7)/7^2}b_1^{-2(j-7)j(j+7)(j+14)/(3\times 7^4)}a_3a_2a_1b_3^{-1}b_2^{-(2j^2-7^2)/7^2} \\
&\quad b_1^{-(2(j/7)^4+8(j/7)^3+4(j/7)^2-8(j/7)-3)/3} \\
&= b_1^{-1}b_1^{-2(j-7)/7}b_1^{-2(j-7)(j+3)/7^2}b_1^{-4(j-7)j(j+7)/(3\times 7^3)}b_1^{-2(j-7)j(j+7)(j+14)/(3\times 7^4)}a_1 \\
&\quad b_1^{-(2(j/7)^4+8(j/7)^3+4(j/7)^2-8(j/7)-3)/3}a_2b_2^{-1}b_2^{-2(j-7)/7}b_2^{-2j(j-7)/7^2}a_2b_2^{-(2j^2-7^2)/7^2} \\
&\quad a_3b_3^{-1}a_3b_3^{-1} \\
&= a_1
\end{aligned}$$

$$\begin{aligned}
x_{j+2} &= a_2b_1^{-2(j-7)/7}b_2^{-1}b_1^{-2(j-7)(j+3)/7^2}a_3b_2^{-2(j-7)/7}b_1^{-4(j-7)j(j+7)/(3\times 7^3)}b_3^{-1}b_2^{-2j(j-7)/7^2} \\
&\quad b_1^{-2(j-7)j(j+7)(j+14)/(3\times 7^4)}a_3a_2a_1b_3^{-1}b_2^{-(2j^2-7^2)/7^2} \\
&\quad b_1^{-(2(j/7)^4+8(j/7)^3+4(j/7)^2-8(j/7)-3)/3}a_1 \\
&= b_1^{-2(j-7)/7}b_1^{-2(j-7)(j+3)/7^2}b_1^{-4(j-7)j(j+7)/(3\times 7^3)}b_1^{-2(j-7)j(j+7)(j+14)/(3\times 7^4)}a_1 \\
&\quad b_1^{-(2(j/7)^4+8(j/7)^3+4(j/7)^2-8(j/7)-3)/3}a_1a_2b_2^{-1}b_2^{-2(j-7)/7}b_2^{-2j(j-7)/7^2}a_2b_2^{-(2j^2-7^2)/7^2} \\
&\quad a_3b_3^{-1}a_3b_3^{-1} \\
&= b_1
\end{aligned}$$

$$
\begin{aligned}
x_{j+3} &= b_2^{-1}b_1^{-2(j-7)(j+3)/7^2}a_3b_2^{-2(j-7)/7}b_1^{-4(j-7)j(j+7)/(3\times 7^3)}b_3^{-1}b_2^{-2j(j-7)/7^2} \\
&\quad b_1^{-2(j-7)j(j+7)(j+14)/(3\times 7^4)}a_3a_2a_1b_3^{-1}b_2^{-(2j^2-7^2)/7^2} \\
&\quad b_1^{-(2(j/7)^4+8(j/7)^3+4(j/7)^2-8(j/7)-3)/3}a_1b_1 \\
&= b_1^{-2(j-7)(j+3)/7^2}b_1^{-4(j-7)j(j+7)/(3\times 7^3)}b_1^{-2(j-7)j(j+7)(j+14)/(3\times 7^4)}a_1 \\
&\quad b_1^{-(2(j/7)^4+8(j/7)^3+4(j/7)^2-8(j/7)-3)/3}a_1b_1b_2^{-1}b_2^{-2(j-7)/7}b_2^{-2j(j-7)/7^2}a_2b_2^{-(2j^2-7^2)/7^2} \\
&\quad a_3b_3^{-1}a_3b_3^{-1} \\
&= a_2b_1^{2j/7}
\end{aligned}
$$

$$
\begin{aligned}
x_{j+4} &= a_3b_2^{-2(j-7)/7}b_1^{-4(j-7)j(j+7)/(3\times 7^3)}b_3^{-1}b_2^{-2j(j-7)/7^2}b_1^{-2(j-7)j(j+7)(j+14)/(3\times 7^4)} \\
&\quad a_3a_2a_1b_3^{-1}b_2^{-(2j^2-7^2)/7^2}b_1^{-(2(j/7)^4+8(j/7)^3+4(j/7)^2-8(j/7)-3)/3}a_1b_1a_2b_1^{2j/7} \\
&= b_1^{-4(j-7)j(j+7)/(3\times 7^3)}b_1^{-2(j-7)j(j+7)(j+14)/(3\times 7^4)}a_1 \\
&\quad b_1^{-(2(j/7)^4+8(j/7)^3+4(j/7)^2-8(j/7)-3)/3}a_1b_1b_1^{2j/7} \\
&\quad b_2^{-2(j-7)/7}b_2^{-2j(j-7)/7^2}a_2b_2^{-(2j^2-7^2)/7^2}a_2a_3b_3^{-1}a_3b_3^{-1} \\
&= b_2b_1^{2j(j+7))/7^2}
\end{aligned}
$$

$$
\begin{aligned}
x_{j+5} &= b_3^{-1}b_2^{-2j(j-7)/7^2}b_1^{-2(j-7)j(j+7)(j+14)/(3\times 7^4)}a_3a_2a_1b_3^{-1}b_2^{-(2j^2-7^2)/7^2} \\
&\quad b_1^{-(2(j/7)^4+8(j/7)^3+4(j/7)^2-8(j/7)-3)/3}a_1b_1a_2b_1^{2j/7}b_2b_1^{2j(j+7))/7^2} \\
&= b_1^{-2(j-7)j(j+7)(j+14)/(3\times 7^4)}a_1b_1^{-(2(j/7)^4+8(j/7)^3+4(j/7)^2-8(j/7)-3)/3}a_1b_1 \\
&\quad b_1^{2j/7}b_1^{2j(j+7))/7^2}b_2^{-2j(j-7)/7^2}a_2b_2^{-(2j^2-7^2)/7^2}a_2b_2b_3^{-1}a_3b_3^{-1} \\
&= a_3b_2^{2j/7}b_1^{4j(j+7)(j+14)/(3\times 7^3)}
\end{aligned}
$$

$$
\begin{aligned}
x_{j+6} &= a_3a_2a_1b_3^{-1}b_2^{-(2j^2-7^2)/7^2}b_1^{-(2(j/7)^4+8(j/7)^3+4(j/7)^2-8(j/7)-3)/3}a_1b_1a_2b_1^{2j/7}b_2 \\
&\quad b_1^{2j(j+7))/7^2}a_3b_2^{2j/7}b_1^{4j(j+7)(j+14)/(3\times 7^3)} \\
&= a_1b_1^{-(2(j/7)^4+8(j/7)^3+4(j/7)^2-8(j/7)-3)/3}a_1b_1b_1^{2j/7}b_1^{2j(j+7))/7^2}b_1^{4j(j+7)(j+14)/(3\times 7^3)} \\
&\quad a_2b_2^{-(2j^2-7^2)/7^2}a_2b_2b_2^{2j/7}a_3b_3^{-1}a_3 \\
&= b_3b_2^{2j(j+7)/7^2}b_1^{2j(j+7)(j+14)(j+21)/(3\times 7^4)}
\end{aligned}
$$

$$
\begin{aligned}
x_{j+7} &= a_1b_1a_2b_1^{2j/7}b_2b_1^{2j(j+7))/7^2}a_3b_2^{2j/7}b_1^{4j(j+7)(j+14)/(3\times 7^3)} \\
&\quad b_3b_2^{2j(j+7)/7^2}b_1^{2j(j+7)(j+14)(j+21)/(3\times 7^4)} \\
&= a_1b_1b_1^{2j/7}b_1^{2j(j+7))/7^2}b_1^{4j(j+7)(j+14)/(3\times 7^3)}b_1^{2j(j+7)(j+14)(j+21)/(3\times 7^4)} \\
&\quad a_2b_2b_2^{2j/7}b_2^{2j(j+7)/7^2}a_3b_3 \\
&= a_3a_2a_1b_3b_2^{(2(j+7)^2-7^2)/7^2}b_1^{(2((j+7)/7)^4+8((j+7)/7)^3+4((j+7)/7)^2-8((j+7)/7)-3)/3}
\end{aligned}
$$

$$
\begin{aligned}
x_{j+8} &= b_1a_2b_1^{2j/7}b_2b_1^{2j(j+7))/7^2}a_3b_2^{2j/7}b_1^{4j(j+7)(j+14)/(3\times 7^3)}b_3b_2^{2j(j+7)/7^2} \\
&\quad b_1^{2j(j+7)(j+14)(j+21)/(3\times 7^4)}a_3a_2a_1b_3b_2^{(2(j+7)^2-7^2)/7^2} \\
&\quad b_1^{(2((j+7)/7)^4+8((j+7)/7)^3+4((j+7)/7)^2-8((j+7)/7)-3)/3} \\
&= b_1b_1^{2j/7}b_1^{2j(j+7))/7^2}b_1^{4j(j+7)(j+14)/(3\times 7^3)}b_1^{2j(j+7)(j+14)(j+21)/(3\times 7^4)}a_1 \\
&\quad b_1^{(2((j+7)/7)^4+8((j+7)/7)^3+4((j+7)/7)^2-8((j+7)/7)-3)/3}a_2b_2b_2^{2j/7}b_2^{2j(j+7)/7^2}a_2 \\
&\quad b_2^{(2(j+7)^2-7^2)/7^2}a_3b_3a_3b_3 \\
&= a_1
\end{aligned}
$$

$$
\begin{aligned}
x_{j+9} &= a_2 b_1^{2j/7} b_2 b_1^{2j(j+7))/7^2} a_3 b_2^{2j/7} b_1^{4j(j+7)(j+14)/(3\times 7^3)} b_3 b_2^{2j(j+7)/7^2} \\
&\quad b_1^{2j(j+7)(j+14)(j+21)/(3\times 7^4)} a_3 a_2 a_1 b_3 b_2^{(2(j+7)^2-7^2)/7^2} \\
&\quad b_1^{(2((j+7)/7)^4+8((j+7)/7)^3+4((j+7)/7)^2-8((j+7)/7)-3)/3} a_1 \\
&= b_1^{2j/7} b_1^{2j(j+7))/7^2} b_1^{4j(j+7)(j+14)/(3\times 7^3)} b_1^{2j(j+7)(j+14)(j+21)/(3\times 7^4)} a_1 \\
&\quad b_1^{(2((j+7)/7)^4+8((j+7)/7)^3+4((j+7)/7)^2-8((j+7)/7)-3)/3} a_1 a_2 b_2 b_2^{2j/7} b_2^{2j(j+7)/7^2} a_2 \\
&\quad b_2^{(2(j+7)^2-7^2)/7^2} a_3 b_3 a_3 b_3 \\
&= b_1^{-1}
\end{aligned}
$$

$$
\begin{aligned}
x_{j+10} &= b_2 b_1^{2j(j+7))/7^2} a_3 b_2^{2j/7} b_1^{4j(j+7)(j+14)/(3\times 7^3)} b_3 b_2^{2j(j+7)/7^2} b_1^{2j(j+7)(j+14)(j+21)/(3\times 7^4)} \\
&\quad a_3 a_2 a_1 b_3 b_2^{(2(j+7)^2-7^2)/7^2} b_1^{(2((j+7)/7)^4+8((j+7)/7)^3+4((j+7)/7)^2-8((j+7)/7)-3)/3} a_1 b_1^{-1} \\
&= b_1^{2j(j+7))/7^2} b_1^{4j(j+7)(j+14)/(3\times 7^3)} b_1^{2j(j+7)(j+14)(j+21)/(3\times 7^4)} a_1 \\
&\quad b_1^{(2((j+7)/7)^4+8((j+7)/7)^3+4((j+7)/7)^2-8((j+7)/7)-3)/3} a_1 b_1^{-1} b_2 b_2^{2j/7} b_2^{2j(j+7)/7^2} a_2 \\
&\quad b_2^{(2(j+7)^2-7^2)/7^2} a_3 b_3 a_3 b_3 \\
&= a_2 b_1^{-2(j+7)/7}
\end{aligned}
$$

$$
\begin{aligned}
x_{j+11} &= a_3 b_2^{2j/7} b_1^{4j(j+7)(j+14)/(3\times 7^3)} b_3 b_2^{2j(j+7)/7^2} b_1^{2j(j+7)(j+14)(j+21)/(3\times 7^4)} \\
&\quad a_3 a_2 a_1 b_3 b_2^{(2(j+7)^2-7^2)/7^2} b_1^{(2((j+7)/7)^4+8((j+7)/7)^3+4((j+7)/7)^2-8((j+7)/7)-3)/3} \\
&\quad a_1 b_1^{-1} a_2 b_1^{-2(j+7)/7} \\
&= b_1^{4j(j+7)(j+14)/(3\times 7^3)} b_1^{2j(j+7)(j+14)(j+21)/(3\times 7^4)} a_1 \\
&\quad b_1^{(2((j+7)/7)^4+8((j+7)/7)^3+4((j+7)/7)^2-8((j+7)/7)-3)/3} \\
&\quad a_1 b_1^{-1} b_1^{-2(j+7)/7} b_2^{2j/7} a_2 a_2 a_3 b_3 a_3 b_3 \\
&= b_2^{-1} b_1^{-2(j+7)(j+14)/7^2}
\end{aligned}
$$

$$
\begin{aligned}
x_{j+12} &= b_3 b_2^{2j(j+7)/7^2} b_1^{2j(j+7)(j+14)(j+21)/(3\times 7^4)} a_3 a_2 a_1 b_3 b_2^{(2(j+7)^2-7^2)/7^2} \\
&\quad b_1^{(2((j+7)/7)^4+8((j+7)/7)^3+4((j+7)/7)^2-8((j+7)/7)-3)/3} a_1 b_1^{-1} a_2 b_1^{-2(j+7)/7} b_2 \\
&\quad b_1^{2(j+7)(j+14)/7^2} \\
&= b_1^{2j(j+7)(j+14)(j+21)/(3\times 7^4)} a_1 b_1^{(2((j+7)/7)^4+8((j+7)/7)^3+4((j+7)/7)^2-8((j+7)/7)-3)/3} \\
&\quad a_1 b_1^{-1} b_1^{-2(j+7)/7} b_2^{2j(j+7)/7^2} a_2 b_2^{(2(j+7)^2-7^2)/7^2} a_2 b_3 a_3 b_3 \\
&= a_3 b_2^{-2(j+7)/7} b_1^{-4(j+7)(j+14)(j+21)/(3\times 7^3)}
\end{aligned}
$$

$$
\begin{aligned}
x_{j+13} &= a_3 a_2 a_1 b_3 b_2^{(2(j+7)^2-7^2)/7^2} b_1^{(2((j+7)/7)^4+8((j+7)/7)^3+4((j+7)/7)^2-8((j+7)/7)-3)/3} \\
&\quad a_1 b_1^{-1} a_2 b_1^{-2(j+7)/7} b_2 b_1^{2(j+7)(j+14)/7^2} a_3 b_2^{-2(j+7)/7} b_1^{-4(j+7)(j+14)(j+21)/(3\times 7^3)} \\
&= a_1 b_1^{(2((j+7)/7)^4+8((j+7)/7)^3+4((j+7)/7)^2-8((j+7)/7)-3)/3} a_1 b_1^{-1} b_1^{-2(j+7)/7} \\
&\quad b_1^{2(j+7)(j+14)/7^2} b_1^{-4(j+7)(j+14)(j+21)/(3\times 7^3)} a_2 b_2^{(2(j+7)^2-7^2)/7^2} a_2 b_2 b_2^{-2(j+7)/7} \\
&= b_3^{-1} b_2^{-2(j+14)(j+7)/7^2} b_1^{-2(j+7)(j+14)(j+21)(j+28)/(3\times 7^4)}
\end{aligned}
$$

$$
\begin{aligned}
x_{j+14} &= a_1 b_1^{-1} a_2 b_1^{-2(j+7)/7} b_2 b_1^{2(j+7)(j+14)/7^2} a_3 b_2^{-2(j+7)/7} b_1^{-4(j+7)(j+14)(j+21)/(3\times 7^3)} \\
&\quad b_3^{-1} b_2^{-2(j+14)(j+7)/7^2} b_1^{-2(j+7)(j+14)(j+21)(j+28)/(3\times 7^4)} \\
&= a_1 b_1^{-1} b_1^{-2(j+7)/7} b_1^{2(j+7)(j+14)/7^2} b_1^{-4(j+7)(j+14)(j+21)/(3\times 7^3)} \\
&\quad b_1^{-2(j+7)(j+14)(j+21)(j+28)/(3\times 7^4)} a_2 b_2 b_2^{-2(j+7)/7} b_2^{-2(j+14)(j+7)/7^2} a_3 b_3^{-1} \\
&= a_3 a_2 a_1 b_3^{-1} b_2^{-(2(j+14)^2-7^2)/7^2} \\
&\quad b_1^{-(2((j+14)/7)^4+8((j+14)/7)^3+4((j+14)/7)^2-8((j+14)/7)-3)/3}
\end{aligned}
$$

So all the above members of the Fibonacci orbit have the required form. Thus the result holds. □

Appendix C

GAP Code

1 The fpfl code and explanations

In this section we give GAP code that calculates the Fibonacci length of a given group. Results from experiments carried out using this code suggested some of the results contained in this thesis.

Before running any programs we first need to change the coset enumerator used by GAP to the more powerful ACE package. This is done via the commands:

```
RequirePackage("ace", "3.0");
TCENUM := ACETCENUM; # This let the more powerful ACE coset enumerator
                     # be used instead of the default enumerator.
```

Below is the code that given a finitely presented group G returns a permutation group isomorphic to G using the internal functions of the ACE package.

```
#########################################################################
##
##  Input:  p a finitely presented group.
```

```
##
##  Output: A permutation group isomorphic to p.
##
permgroup:=function(p)
local table, # the coset table of p calculated using ACE
      pgens, # a list of permutation generators
      tg,    # the size of the coset table
      i,     # a loop variable
      test;  # a possibly new permutation generator

if not IsFpGroup(p) then
        return Print("Error in permgroup","\n");
fi;
table:=CosetTableFromGensAndRels(FreeGeneratorsOfFpGroup(p),
                RelatorsOfFpGroup(p), [ ] : wo:=2*10^8);;
pgens:=[ ];;
tg:=Length(table);;
for i in [1..tg] do
        test:= PermList(table[i]);
                if not test^(-1) in pgens then Add(pgens, test); fi;
od;

return Group(pgens);
end;
```

Now we introduce a program that will calculate the basic Fibonacci length of a given group G generated by the finite tuple A. The basic Fibonacci length may be calculated by finding the smallest value k, $k \geq 2$, satisfying

$$|x_1| = |x_k|, |x_2| = |x_{k+1}|, ..., |x_k| = |x_{2k-1}|$$

where x_i is the *ith* entry in the Fibonacci orbit of G using the generating set A.

```
#####################################################################
##
##  Input:  p a group
##
##  Output: the basic Fibonacci length of p
##
blen:=function(p, stop)
local gens,          # generators of the group p
      nogens,        # the number of generators of p
      memory,        # a list of elements of the Fibonacci orbit
      listoforders, # a list of the orders of the generators of p
      i, bool, k,    # loop variables
      newel,         # a new element to be tested
      halflength,    # half the length of listoforders
      stopping;      # the number of elements of the Fibonacci
                     # orbit to be calculated

gens:=GeneratorsOfGroup(p);
nogens:=Length(gens);
memory:=ShallowCopy(gens);
listoforders:=List([1..nogens], x->Order(gens[x]));

for i in [1..nogens] do
         Print(i," ", Order(gens[i]), "\n");
```

```
od;

bool:=false;
stopping:=nogens+1;

while  bool = false do
        newel:= Product(memory);
        Print(stopping," ", Order(newel), "\n");

        memory:=List([1..nogens - 1], i->memory[i+1]);
        Add(memory,newel);

        Add(listoforders,  Order(newel));

        if IsEvenInt(Length(listoforders)) then
                halflength:=(Length(listoforders))/2;
                k:=0;;
                while k < halflength do
                        k:=k+1;
                        if not listoforders[k] =
                             listoforders[k+halflength] then
                                k:=halflength+7;
                        fi;
                od;
                if k = halflength then
                        bool :=true;
                        Print("The basic Fibonacci length is ");
                        return halflength;
                fi;
```

```
        fi;

        stopping:=stopping+1;
        if stopping = stop then bool :=true;
                Print("Stopping condition has halted the program ");
                return 0;
        fi;
od;

end;
```

The following code will calculate the Fibonacci length of a finitely presented group or will stop when a prespecified number of elements of the Fibonacci orbit has been calculated. The code is fastest if the input group is a permutation group.

```
#########################################################################
##
##  Input:  p a group, stop the number of steps of the Fibonacci
##          length that is to be calculated
##
##  Output: The Fibonacci length or a message saying that the stop
##          limit has been reached
##
len:= function(p, stop)
local gens, # generators of the group p
nogens,     # the number of generators of p
memory,     # a list of nogens elements of the Fibonacci orbit of p
fiblength,  # The Fibonacci length plus the number nogens
```

```
temp,       # loop variable
stopping,   # the number of elements of the Fibonacci orbit to be calculated
newel;      # the latest element of the Fibonacci orbit of p

if IsCyclic(p) then
return Wall(Size(p));
fi;

gens:=GeneratorsOfGroup(p);
nogens:=Length(gens);
memory:=ShallowCopy(gens); # This will store the last nogens
                           # elements of the Fibonacci orbit
fiblength:=nogens;
temp:=1;
stopping:=nogens;

while not temp = nogens+1 do
        newel:= Product(memory);        #The next element in the sequence.
        fiblength := fiblength+1;

        if newel = gens[temp] then
                temp := temp + 1;
        else
                temp:=1;
        fi;
        memory:=List([1..nogens - 1], i->memory[i+1]);
                                                # This updates the
                                                # memory list to include
                                                # the youngest element,
```

```
        Add(memory,newel);                          # and exclude the oldest.
        if not stop=0 then # Advance the variable stopping on by one
                stopping:=stopping+1;
        fi;
        if stopping = stop then
                temp := nogens+1;
                Print("Stopping condition has halted the program ");
                return 0;
        fi;

od;

return (fiblength - nogens);
end;
```

Below is the code that chooses which program to call, either the Fibonacci , the basic Fibonacci or both.

```
#########################################################################
##
##  Input:  g a group, c the choice of result either the Fibonacci
##          length, the basic Fibonacci length or both, s the
##          number of steps in the orbits required.
##  Output: the requested result.
##
FibLengths:= function(g, c, s)
local b, l;

if c = "b"  and IsFpGroup(g) then return blen(permgroup(g),s);
```

```
 elif c = "b" then return blen(g,s);
fi;

if c = "l" and IsFpGroup(g) then return len(permgroup(g), s);
 elif c = "l" then return len(g,s);
fi;

if c = "bl" and IsFpGroup(g) then
        b:=blen(permgroup(g),s);;
        l:=len(permgroup(g),s);;
        Print("\n", "\n");
        return [b, l];
 elif c = "bl" then return [blen(g,s), len(g,s)];
fi;

end;
```

1.1 Examples

Below we give examples of how the above programs were used to generate results that appear in this thesis.

```
gap> f:=FreeGroup(2);; a:=f.1;; b:=f.2;;
gap> rels:=[a*b*a^(-1)*b^(-51), b*a*b^(-1)*a^(-51)];;
gap> g:=f/rels;;
gap> FibLengths(g,"l",0);
7500
gap> time;
126610
```

```
gap> f:=FreeGroup(2);; a:=f.1;; b:=f.2;;
gap> rels:=[(a*b)^(185)*a*b^(-1), (b*a)^(185)*b*a^(-1)];;
gap> g:=f/rels;;
gap> FibLengths(g,"l",0);
1200
gap> time;
23130

gap> f:=FreeGroup(4);; a:=f.1;; b:=f.2;; c:=f.3;; d:=f.4;;
gap> rels:=[a^2, b^7, (a*b)^(2), c^2, d^7, (c*d)^2,
Comm(a,c), Comm(a,d), Comm(b,c), Comm(b,d)];;
gap> g:=f/rels;;
gap> FibLengths(g,"l",0);
70
gap> time;
140
```

2 Wall numbers

Here we present two programs that will calculate the Wall number of a given positive integer.

The program K will calculate the Wall number of a given prime number p. It uses results from [70] once the rank of apparition is found.

```
#########################################################################
##
##  Input:  p a prime number
##
##  Output: the Wall number of p
##
K:=function(p)
local seq, # the Fibonacci sequence modulo p
l;         # the length of seq

if p=2 then return 3; fi; # K(2)=3

if not (IsPrimeInt(p)) then
Print("The input is not a prime number, \n");
return 0;
fi;

seq:=[0,1];
while not ((seq[Length(seq)-1]+seq[Length(seq)]) mod p = 0) do
        Add(seq, (seq[Length(seq)-1]+seq[Length(seq)]) mod p );
od;
# we have just checked that not(seq[i]+seq[i+1] = 0 mod p)

l:=Length(seq);

if IsOddInt(l) then
        return 4*l;
elif seq[Length(seq)]=1 then
        return l;
```

```
else
        return 2*l;
fi;

end;
```

The following program calculates the Wall number of any positive integer. The program assumes that $k(p^2) = pk(p)$, where p is an odd prime; this has been checked for all primes p where $p < 10^9$.

```
#########################################################################
##
##  Input:  n a positive integer
##
##  Output: the Wall number of n
##
Wall:=function(n)
local decom, # a factorization of n into primes and their powers
h_i,         # a list of k(p) for primes p
i,           # a loop variable
kp,          # k(p) for a prime p
kpn;         # p^(n-1)*k(p) the use of the Wall conjecture

decom:=PrimePowersInt(n);
h_i:=[ ];;

for i in [1..Length(decom)/2] do
        kp:=K(decom[2*i-1]);
        kpn:=decom[2*i-1]^(decom[2*i]-1)*kp;
```

```
        Add(h_i, kpn);
od;

return Lcm(h_i);
end;
```

2.1 Examples

Here we present some examples of the use of the above programs to show how they work and to illustrate the speed of the algorithms (all times are milliseconds of CPU time).

```
gap> Wall(11);;
gap> time;
0

gap> Wall(Product(Primes));; # The product of the first 168 primes
1323493546245402879451495701646743565937838464105706596737402460\
9735288543009156410576774425754848000
gap> time;
400

gap> x:=Random(Primes)^(Random(Primes))*Random(Primes)^(Random(Primes));;
gap> PrimePowersInt(x);
[ 349, 373, 797, 883 ] # so x=349^(373)*797^(883)
gap> time;
6560
gap> Wall(x);;
gap> time;
```

```
6620

gap> x:=Random(Primes)^(Random(Primes))*Random(Primes)^(Random(Primes));;
gap> PrimePowersInt(x);
[ 727, 1140 ] # so x=727^(1140)
gap> time;
6090
gap> Wall(x);;
gap> time;
6100
```

As can be seen from the above examples most of the time needed to complete the computation is spent factorizing the given number.

Table of notation

$\mathbb{N}$	the natural numbers $\{1, 2, 3, \ldots\}$
$\mathbb{Z}$	the integers
$\mathbb{Z}_p$	the additive cyclic group of order p
$\mathbb{Z}_p^*$	the multiplicative group of order $p-1$
$GF(p)$	the field of order p
$\Phi(G)$	the Frattini subgroup of G
$\phi(n)$	Euler's Totient
G'	$\langle\, [x,y] \,:\, x,y, \in G \,\rangle$
G/N	the group G factored out by the normal subgroup N
$\overline{R}$	the normal closure of the set R
$LEN_X(G)$	the Fibonacci length of G with respects to the set X
$(\frac{a}{p})$	the Legendre symbol
$\lfloor x \rfloor$	the largest integer less than or equal to x
f_n	the nth Fibonacci number
g_n	the nth Lucas number
$M(G)$	the Schur multiplier of the group G
$G \times H$	the direct product of the groups G and H
$G \otimes H$	the tensor product of the groups G and H
$G * H$	the free product of the groups G and H
$G \ltimes H$	the semidirect product of the groups G and H
C_n	the cyclic group of order n

$d(G)$	the rank of G
$Z(G)$	the centre of the group G
$\|G\|$	the order of G
$F(X)$	the free group on the set X
$\mathrm{def}(G)$	the deficiency of the group G
$\mathrm{def}(\mathcal{P})$	the deficiency of the presentation $\mathcal{P}$
$a\|b$	a divides b
$\mathrm{Im}(f)$	the image of f
$\mathrm{Ker}(f)$	the kernel of f
D_∞	the infinite dihedral group
$k(n)$	the Wall number of n
(a, b)	the greatest common divisor of a and b
$\begin{pmatrix} a \\ b \end{pmatrix}$	the binomial coefficient $\frac{a!}{b!(a-b)!}$
$\phi_n(G)$	Hall's Euler function of the group G on n generators
$\{\mathrm{id}\}$	the trivial group
1	the group identity element
$\mathrm{ra}(n)$	the rank of apparition of n
$\mathrm{t}(n)$	$k(n)/\mathrm{ra}(n)$
$N \lhd G$	N is a proper normal subgroup of G
$N \leq G$	N is a subgroup of G
$F_k(G; X)$	the k-nacci sequence of G with seed set X
$[x, y]$	the commutator $x^{-1}y^{-1}xy$

Bibliography

[1] bin Ahmad, A. G., *The unsolvability of efficiency for groups*, Southeast Asia Bull. Math. **22** (1998), 331-336.

[2] Andrews, G. H., *Some formulae for the Fibonacci sequence with generalizations*, Fibonacci Quart. **7** (1969), 113-130.

[3] Aydin, H. and Dikici, R., *General Fibonacci sequences in finite groups*, Fibonacci Quart. **36** (1998), 216-221.

[4] Aydin, H. and Smith, G. C., *Finite p-quotients of some cyclically presented groups*, J. London Math. Soc. **49** (1994), 83-92.

[5] Ayik, H., *Presentations and efficiency of semigroups* (Ph.D. Thesis, University of St Andrews, Scotland, 1998).

[6] Ayik, H., Campbell, C. M., O'Connor, J. J. and Ruškuc, N., *The semigroup efficiency of direct powers of groups*, in *Semigroups Braga 1999* (eds: Smith, P, Giraldes, E. and Martins, P., World Scientific Publishing Co., River Edge NJ, 2000), 19-25.

[7] Ayik, H., Campbell, C. M., O'Connor, J. J. and Ruškuc, N., *The semigroup efficiency of groups and monoids*, Math. Proc. R. Ir. Acad. **100A** (2000), 171-176.

[8] Bach, E., *Comments on search procedures for primitive roots*, Math. Comp. **66** (1997), 1719-1727.

[9] Bechtell, H., *Elementary groups*, Trans. Amer. Math. Soc. **114** (1965), 355-362.

[10] Bechtell, H., *Inseparable finite solvable groups*, Trans. Amer. Math. Soc. **216** (1976), 47-60.

[11] Benson, C. T. and Mendelsohn, N. S., A *calculus for a certain class of word problems in groups*, J. Comb. Theory **1** (1966), 202-208.

[12] Beyl, F. R., *The Schur multiplicator of metacyclic groups*, Proc. Amer. Math. Soc. **40** (1973), 313-318.

[13] Beyl, F. R. and Jones, M.R., *Addendum to 'The Schur multiplicator of metacyclic groups'*, Proc. Amer. Math. Soc. **43** (1974), 251-252.

[14] Brookes, M. J., Campbell, C. M. and Robertson, E. F., *Efficiency and direct products of groups*, in *Groups-Korea 94* (eds: Kim, A. C. and Johnson, D. L., Walter de Gruyter & Co., Berlin, New York, 1995), 277–284.

[15] Campbell, C. M., lecture notes, private communication.

[16] Campbell, C. M., Campbell, P. P., Doostie, H. and Robertson, E. F., *Fibonacci length for certain metacyclic groups*, Algebra Colloq., to appear.

[17] Campbell, C. M., Campbell, P. P., Doostie, H. and Robertson, E. F., *On the Fibonacci length of powers of dihedral groups*, Vol 9, in *Applications of Fibonacci numbers* (ed: Howard, F. T., Kluwer Academic Press, The Netherlands), to appear.

[18] Campbell, C. M., Campbell, P. P., Hopson, B. T. K. and Robertson, E. F., *On the efficiency of direct powers of PGL(2,p)*, in *Group theory and low-*

dimensional topology, German-Korean workshop, Pusan 2000 (eds: Mennicke, J. and Cho, J. R., Research and exposition in Mathematics, Vol 27, Heldermann Verlag), to appear.

[19] Campbell, C. M., Doostie, H. and Robertson, E. F., *Fibonacci length of generating pairs in groups*, in *Applications of Fibonacci numbers*, Vol. 3, (eds: Bergum, G.A., *et al*, Kluwer Academic Press, 1990), 27-35.

[20] Campbell, C. M., Miyamoto, I., Robertson, E. F. and Williams, P. D., *The efficiency of $PSL(2,p)^3$ and other direct products of groups*, Glasgow Math. J. **39** (1997), 259-268.

[21] Campbell, C. M. and Robertson, E. F., *On a group presentation due to Fox*, Canad. Math. Bull. **19** (1976), 247-248.

[22] Campbell, C. M., Robertson, E. F. and Williams, P. D., *On the efficiency of some direct powers of groups*, in *Groups-Canberra 1989*, (ed: Kovács, L. G., Lecture Notes in Math. **1456** Springer, Berlin, 1990), 106-113.

[23] Campbell, C. M., Robertson, E. F. and Williams, P. D., *Efficient presentations of direct powers of imperfect groups*, Algebra Colloq. **4** (1997), 21–27.

[24] Chalk, C. P., and Johnson, D. L., *The Fibonacci Groups. II*, Proc. Roy. Soc. Edinburgh **77** (1977), 79-86.

[25] Cohen, S. D., *Pairs of primitive roots*, Mathematika **32** (1985), 276-285.

[26] Cohen, S. D., *Primitive elements and polynomials : existence results*, in *Finite fields, coding theory, and advances in communications and computing*, (eds: Mullen, G. L. and Shiue, P. J-S., Lecture Notes in Pure and Applied Mathematics **141** Marcel Dekker), 43-55.

[27] Cohen, S. D., private communication.

[28] Conway, J. H., *Advanced problem 5327*, Amer. Math. Monthly **72** (1965), 915.

[29] Conway, J. H., *et al*, *Solution to advanced problem 5327*, Amer. Math. Monthly **74** (1967), 91-93.

[30] Doostie, H., *Fibonacci-type sequences and classes of groups* (Ph.D. Thesis, University of St Andrews, Scotland, 1988).

[31] Doostie, H. and Campbell, C.M., *Fibonacci length of automorphism groups involving Tribonacci numbers*, Vietnam J. Math. **28** (2000), 57-65.

[32] Doostie, H. and Golamie, R., *Computing on the Fibonacci lengths of finite groups*, Int. J. Appl. Math. **4** (2000), 149-156.

[33] Droubay, X. and Pirillo, G., *Palindromes and Sturmian words*, Theoret. Comput. Sci. **223** (1999), 73-85.

[34] Erdős, P., *Some unconventional problems in number theory*, Acta Math. Acad. Sci. Hungar. **33** (1979), 71-80.

[35] Erdős, P., Graham, R. L., Ruzsa, I. and Straus, E. G., *On the prime factors of* $\begin{pmatrix} 2n \\ n \end{pmatrix}$, Math. Comp. **29** (1975), 83-92.

[36] GAP, *GAP-Groups, Algorithms, and Programming, Version 4.3*, Aachen, St.-Andrews, 2002. (`http://www.gap-system.org`)

[37] Goetgheluck, P., *On prime divisors of binomial coefficients*, Math. Comp. **54** (1988), 325-329.

[38] Hall, P., *The Eulerian function of a group*, Quart. J. Math **7** (1936), 134-151.

[39] Harlander, J., *Some aspects of efficiency* in *Groups-Korea 98 (Pusan)* (eds: Baik, Y. G., Johnson, D. L. and Kim, A. C., Walter de Gruyter & Co., Berlin, New York, 2000), 165-180.

[40] Hert, T. and Williams, P. D., *A note on a presentation of* $PGL(2,p)$, to appear.

[41] Hopf, H., *Fundamentalgruppe und zweite Bettische Gruppe*, Comment. Math. Helv. **14** (1942), 257-309.

[42] Hungerford, T. W., *Algebra* (Graduate Texts in Math. **73**, Springer-Verlag, New York, 1974).

[43] Huppert, B., *Endliche Gruppen 1* (Springer, Berlin, 1967).

[44] Jefford, A., *A quest for autumnal repose*, Decanter **10** 2002, 16.

[45] Johnson, D. L., *Presentations of groups*, 2nd edition (London Math. Soc. Student Texts **15**, Cambridge University Press, Cambridge 1997).

[46] Johnson, D. L., Walmsley, J. W. and Wright, D., *The Fibonacci groups*, Proc. London Math. Soc. **29** (1974), 577-592.

[47] Karpilovsky, G., *The Schur multiplier* (London Math. Soc. Monographs New Series **2**, Clarendon Press, Oxford 1987).

[48] Knox, S. W., *Fibonacci sequences in finite groups*, Fibonacci Quart. **30** (1992), 116-120.

[49] Knuth, D. E. and Bendix, P. B., *Simple word problems in universal algebra*, in *Computational problems in abstract algebra* (ed: Leech, J., Pergamon Press, Oxford, 1970), 263-297.

[50] Luca, A. de, *A combinatorial property of the Fibonacci words*, Inform. Process. Lett. **12** (1981), 193-195.

[51] Mitchell, J. D., *Extremal problems in combinatorial semigroup theory* (Ph.D. Thesis, University of St Andrews, Scotland, 2002).

[52] Newman, M. F., *Proving a group infinite*, Arch. Math. (Basel) **54** (1990), 209-211.

[53] Niederreiter, H., *Distribution of Fibonacci numbers modulo* 5^k, Fibonacci Quart. **10** (1972), 373-374.

[54] Neubüser, J., *An elementary introduction to coset table methods in computational group theory*, in *Groups-St Andrews 1981* (eds: Campbell, C. M. and Robertson, E. F., London Math. Soc. Lecture Notes **71**, Cambridge University Press, Cambridge, 1982), 137–154.

[55] Robertson, E. F. and Williams, P. D., *A presentation of* $PGL(2,p)$ *with three defining relations*, Proc. Edinburgh Math. Soc. **27** (1984), 145-149.

[56] Robinson, D. J. S., *A course in the theory of groups* (Springer-Verlag, New York, 1982).

[57] Robinson, D. W., *A note on linear recurrent sequences modulo m*, Amer. Math. Monthly **73** (1966), 619-621.

[58] Rotman, J. J., *An introduction to the theory of groups*, fourth edition (Springer-Verlag, New York, 1995).

[59] Rozenberg, G., *Theory of L systems: from the point of view of formal language theory*, in *L Systems* (eds: Goos, G. and Hartmanis, J., Lecture notes in Computer Science **15**, Springer-Verlag, 1974), 1-23.

[60] Ruškuc, N., *Semigroup presentations* (Ph.D. Thesis, University of St Andrews, Scotland, 1996).

[61] Sárközy, A., *On divisors of binomial coefficients,* I, J. Number Theory **15** (1985), 70-80.

[62] Sims, C. C., *Computation with finitely presented groups* (Encyclopedia of mathematics and its applications **48**, Cambridge University Press, Cambridge, 1994).

[63] Sun, Z-H and Sun, Z-W, *Fibonacci numbers and Fermat's last theorem*, Acta. Arith. **60** (1992), 371-388.

[64] Thomas, R. M., *The Fibonacci groups revisited*, in *Groups-St Andrews 1989* Vol 2 (eds: Campbell, C. M. and Robertson, E. F., London Math. Soc. Lecture Notes **160**, Cambridge University Press, Cambridge, 1991), 445-454.

[65] Todd, J. A. and Coxeter, H. S. M., *A practical method for enumerating cosets of a finite abstract group*, Proc. Edinburgh Math. **5** (1936), 26-34.

[66] Yu, S. S. and Zhao, Y-K, *Properties of Fibonacci languages*, Discrete Math. **224** (2000), 215-223.

[67] Vajda, S., *Fibonacci & Lucas numbers, and the golden section* (Ellis Horwood, Chichester, 1989).

[68] Vegh, E., *A note on the distribution of the primitive roots of a prime*, J. Number Theory **3** (1971), 13-18.

[69] Vinogradov, I. M., *Elements of number theory* (Dover Publications, New York, 1954).

[70] Vinson, J., *The relation of the period modulo to the rank of apparition of m in the Fibonacci sequence*, Fibonacci Quart. **2** (1963), 37-45.

[71] Wall, D. D., *Fibonacci series modulo m*, Amer. Math. Monthly **67** (1960), 525-532.

[72] Wiegold, J., *Growth sequences of finite groups* III, J. Austral. Math. Soc. **25** (1978), 142-144.

[73] Wiegold, J., *The Schur multiplier*, in *Groups-St Andrews 1981* (eds: Campbell, C. M. and Robertson, E. F., London Math. Soc. Lecture Notes **71**, Cambridge University Press, Cambridge, 1982), 137–154.

[74] Wilcox, H. J., *Fibonacci sequences of period n in groups*, Fibonacci Quart. **4** (1986), 356-361.

[75] Williams, H. C., *A note on the Fibonacci quotient* $F_{p-\epsilon}/p$, Canad. Math. Bull. **25** (1982), 366-370.

[76] Zhang, G-Q., *Automata, boolean matrices, and ultimate periodicity*, Inform. and Comput. **152** (1999), 138-154.